Polizeiliche Datenverarbeitung zur Gefahrenabwehr

Von Prof. Dr. **Christoph Gusy**, Bielefeld*

Polizeiliche Gefahraufklärung erschöpft sich nicht in Maßnahmen der Informationserhebung gegen Grundrechtsträger. In den meisten Fällen fängt sie erst danach eigentlich an: Ist die angetroffene Person mit einer gesuchten identisch? Finden sich ihre Spuren an einem Drohbrief? Ist der angetrunkene Fußballfan ein Hooligan? Hier geht es um die Verarbeitung erhobener Daten. Sie kann ihrerseits grundrechtlich relevant sein.

I. Grundrechtsrelevante Informationsverarbeitung

1. Gefahrenabwehr als Informationsverarbeitung

Polizeiliche Aufgabenerfüllung besteht in hohem Maße aus Informationsverarbeitung. Sie ist in Gesetzen partiell eigenständig geregelt, partiell aber auch lediglich vorausgesetzt. Jeder behördliche Grundrechtseingriff zur Gefahrenabwehr[1] oder zur Ahndung einer Straftat setzt voraus, dass „tatsächliche Anhaltspunkte" für das Vorliegen einer Gefahr oder den Verdacht einer Straftat bestehen; anders ausgedrückt: dass die zur Aufklärung notwendigen Tatsachen jedenfalls insoweit geklärt sind. Diese Klärung ist Informationsverarbeitung. Sie schafft die gesetzlich statuierten Zulässigkeitsvoraussetzungen weiterer Maßnahmen. Aufklärung ist im Gefüge staatlicher Aufgabenerfüllung insoweit kein Selbstzweck; sie hat vielmehr dienende Funktion.[2] Es ist der Zweck der Gefahrenabwehr bzw. Strafverfolgung, welche die vorgelagerten Informationseingriffe rechtfertigt und zugleich begrenzt. In diesem Kontext kann Informationsverarbeitung der Gewinnung oder der Überprüfung von Gefahr- bzw. Verdachtshypothesen dienen. Sie kann auf ganz unterschiedliche Weise erfolgen: Entweder im Kopf des Polizeibeamten (dies ist gar nicht selten), oder aber mithilfe des Wissens anderer Personen oder Dienststellen, aber auch (immer häufiger) mittels elektronisch gespeicherter Daten oder aber (immer seltener, aber noch vielfach relevant) aus schriftlich fixierten Unterlagen, also aus Akten. Sie kann rasch – durch bloßes Kombinieren im Kopf – oder gründlicher, gar formalisiert im Verwaltungsverfahren erfolgen. Und sie kann vom entscheidenden Beamten allein oder aber mithilfe Dritter, ggf. auch außenstehender Personen, etwa privater Auskunftspersonen oder entscheidungsbefugter Richter, erfolgen. Ob und wie sie erfolgt, hängt keineswegs stets allein von den vorhandenen Informationen ab. Mindestens ebenso wichtig sind andere Umstände, etwa die Verfügbarkeit von Informationen zu einem konkreten Zeitpunkt – sind bestimmte Personen erreichbar, bestimmte Behörden geöffnet, bestimmte Dateien abrufbar? – oder die jeweils aufzuklärende Gefahr: Bedarf es im Falle ihres Vorliegens eines sofortigen Eingreifens oder kann die Aufklärung auch längere Zeit in Anspruch nehmen, ohne dass der Schaden irreparabel eintritt?

Welche Informationen benötigt werden, hängt demnach mindestens von zwei Faktoren ab: Von den im Einzelfall vorhandenen Informationen einerseits und den für mögliche behördliche Maßnahmen notwendigen Informationen andererseits. Fallen beide Informationsmengen zusammen, so sind keine weiteren Aufklärungen erforderlich. Vielfach ist dies jedoch nicht der Fall: In solchen Fällen bestimmt die möglicherweise anzuwendende Norm die Richtung weiterer Aufklärung.[3] Dann geht es also um die Erlangung der für die Tatbestandserfüllung notwendigen Daten und deren Überprüfung im Hinblick darauf, ob die Tatbestandsvoraussetzungen im Einzelfall erfüllt sind oder nicht. An diese Prüfung schließt sich dann die Entscheidung über den Einsatz bzw. Nichteinsatz des jeweiligen Gefahrbeseitigungseingriffs[4] an.

Die polizeiliche Informationsverarbeitungsaufgabe geht jedoch über den geschilderten Kontext hinaus. Sie beginnt nicht erst im Zeitpunkt der Entscheidung über einen konkreten Einsatz, sondern setzt bereits früher an, um für den Einsatzzeitpunkt die notwendigen Informationen verfügbar zu machen und zu halten. Wenn jemand Sachen anbietet, die Hehlerware sein könnten, so wäre es unzweckmäßig, jetzt erst mit der Frage danach zu beginnen, ob irgendwo etwas gestohlen worden ist und ob diese Sachen mit den dort gestohlenen identisch sein könnten. Bis dies geklärt ist, ist die Ware abgesetzt oder der Anbieter verschwunden. Daher müssen die relevanten Informationen über Diebstähle und gestohlene Sachen zeitnah und schnell verfügbar sein. Dazu bedarf es einer Informationsinfrastruktur,[5] welche die notwendigen Angaben verfügbar macht und rasch zur Verfügung stellen kann. Aufbau und Pflege dieser Infrastruktur sind u.a. gemeint, wenn der Polizei zur Aufgabe gemacht ist, „die erforderlichen Vorbereitungen für die Hilfeleistung und das Handeln in Gefahrfällen zu treffen"[6]. Dazu reichen nicht irgend-

---

* Der *Verf.* ist Inhaber des Lehrstuhls für Öffentliches Recht, Staatslehre und Verfassungsgeschichte an der Universität Bielefeld. Für umsichtige und tatkräftige Mitarbeit dankt er Frau *C. Bendisch*, Bielefeld.

[1] Zur Unterscheidung von Gefahraufklärungs- und Gefahrabwehreingriffen *Gusy*, Polizei- und Ordnungsrecht, 7. Aufl. 2009, Rn. 179 ff. einerseits, Rn. 276 ff. andererseits; *Schenke*, Polizei- und Ordnungsrecht, 6. Aufl. 2009; Rn. 9 ff.; *Würtenberger/Heckmann*, Polizeirecht in Baden-Württemberg, 6. Aufl. 2005, Rn. 33 ff.

[2] Näher *Gusy*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts II, 2008, § 23 Rn. 33 ff.

[3] Zur Informationserhebung *Gusy*, JA 2011, 641.

[4] Soweit hierbei Ermessen eingeräumt ist, dient die Informationsverarbeitung auch der Aufklärung der Frage nach möglichen Ermessensbindungen.

[5] Zu solchen Infrastrukturen *Ladeur*, in: Hoffmann-Riem u.a. (Fn. 2), § 21, zur Kommunikationsinfrastruktur näher Rn. 77 ff.; zur elektronischen Infrastruktur ebd., Rn. 85 ff.; ganz grundlegend *Fassbender*, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts, Bd. 4, 3. Aufl. 2006, § 76.

[6] Siehe § 1 Abs. 1 S. 2 NRWPolG; s.a. § 1 Abs. 5 S. 2 i.V.m. §§ 9 f., 11 ff., 26 ff., 32 f. NRWPolG. Zur Auslegung dieser Vorschriften s. insb. *Würtenberger/Heckmann* (Fn. 1), Rn. 538, 586 ff.; ferner *Schoch*, in: Schmidt-Aßmann/Schoch (Hrsg.),

welche Informationen oder -sammlungen aus. Vielmehr müssen diese auch nutzbar sein, insbesondere den praktischen Anforderungen der Vollständigkeit, der Verfügbarkeit und der Aktualität der Informationen entsprechen. Ob sie diese Anforderungen erfüllen, richtet sich nicht zuletzt nach den maßgeblichen rechtlichen Vorgaben. Schon deshalb tritt als weitere Anforderungen diejenige der Rechtmäßigkeit der Bestände hinzu.

2. Grundrechtsrelevanz der Informationsverarbeitung

Nicht jede polizeiliche Informationsverarbeitung ist grundrechtsrelevant. Soweit sie sich auf allgemeine Lagen, Sachen oder Spuren beziehen und keine Zuordnung zu bestimmten Personen ermöglichen, ist ihre Verarbeitung im Einzelfall ebenso wie in der Informationsinfrastruktur grundrechtsneutral und unterliegt allein den allgemeinen Anforderungen an staatliche Datenverarbeitung. Einen Bezug zu geschützten Rechten erlangen Daten nicht durch die Form ihrer Verarbeitung – elektronisch, schriftlich oder auf sonstige Weise –, sondern durch ihren Inhalt. Soweit sie Aussagen über bestimmbare natürliche oder juristische Personen ermöglichen, also personenbezogene Informationen enthalten[7], sind sie grundrechtsrelevant. Auch wenn es hier manche Abgrenzungsschwierigkeiten geben kann[8] und auch nicht jede der Daten in gleicher Weise schutzwürdig sein mag, so ist doch weitestgehend anerkannt: Der Personenbezug begründet den Grundrechtsbezug.

Dies gilt auch für Daten, welche bereits erhoben sind, sich also im Kenntnisbereich der öffentlichen Gewalt befinden. Ihre weitere Verarbeitung stellt einen zusätzlichen Informationseingriff dar, der geeignet ist, den durch die Ermittlung der Information stattgefundenen Eingriff zu vertiefen. Weder rechtfertigt die Erhebung jede weitere Verarbeitung, noch ist jede Verarbeitung eine bloße Fortsetzung der Erhebung. Das gilt namentlich – aber nicht nur – dann, wenn ein Datum zu einem bestimmten Zweck erhoben worden ist, aber zu einem anderen Zweck genutzt werden soll. In solchen Fällen kann der Erhebungszweck nicht die Verarbeitung rechtfertigen und der Verarbeitungszweck nicht die Erhebung. Von daher gilt der wichtige Grundsatz der Zweckbindung erhobener Daten: Informationen dürfen zu dem Zweck verarbeitet werden, zu dem sie erhoben worden sind.[9] Zumindest jede Nutzung zu anderen Zwecken stellt einen Folgeeingriff gegenüber dem ursprünglichen Erhebungsvorgang dar.[10] Aber auch dann, wenn in der Erhebung der Daten kein Eingriff lag, sie also etwa von Betroffenen freiwillig oder gar auf eigene Initiative angegeben worden sind, so ist doch jede Zweckentfremdung im staatlichen Bereich ein (neuer) Grundrechtseingriff.

Dessen Schwere folgt zunächst aus dem Umstand, dass die Datenverarbeitung ein allein interner Vorgang ist, welcher vom Betroffenen weder erkennbar noch kontrollierbar ist. Wirksamer, insbesondere zeitgerechter Rechtsschutz ist folglich regelmäßig unmöglich; ein Zustand, der zumindest mit dem Zweck des Art. 19 Abs. 4 GG schwer vereinbar ist. Vielmehr erfahren Betroffene von dem Verarbeitungsvorgang frühestens dann, wenn eine staatliche Maßnahme ihnen gegenüber auf die verarbeitete Information gestützt wird, wenn also etwa aufgrund von Angaben gegenüber dem Finanzamt polizeiliche Ermittlungsmaßnahmen eingeleitet werden. Zu diesem Zeitpunkt sind vollendete Tatsachen geschaffen, der Datenübermittlungsvorgang war dann rechtsschutzlos. Daneben richtet sich die Schwere des Eingriffs auch nach den betroffenen Daten, ob diese ohnehin allgemein bekannt, zur öffentlichen Bekanntgabe bestimmt sind, oder aber umgekehrt einem besonderen Geheimnisschutz unterliegen[11] bzw. nahe am Kernbereich der Privatsphäre angesiedelt sind.[12]

Entsprechend der allgemeinen polizeilichen Aufgabendifferenzierung ist auch die Informationsverarbeitung in unterschiedlichen Gesetzen geregelt:

a) Maßnahmen zur Aufklärung und Aburteilung von Straftaten richten sich zentral nach §§ 151 ff. StPO; die Informationsverarbeitung zu diesem Zweck nach §§ 474 ff. StPO.[13] Diese gelten nicht nur für gerichtliche und staatsanwaltschaftliche, sondern auch für polizeiliche Ermittlungshandlungen. Geregelt sind die Speicherung, Nutzung und

Besonderes Verwaltungsrecht, 14. Aufl. 2008, Kap. 2 Rn. 12 ff.

[7] Dazu *Dammann*, in: Simitis (Hrsg.), BDSG, 7. Aufl. 2011, § 3 Rn. 3 ff.; *Petri*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2007, H Rn. 2; *Schenke* (Fn. 1), Rn. 176.

[8] Hierzu am Beispiel von Google-Street-View *Holznagel/Schumacher*, JZ 2011, 57; *Caspar*, DÖV 2009, 965; *Dreier/Spiecker* (Hrsg.), Die systematische Aufnahme des Straßenbilds, 2010.

[9] § 23 Abs. 1 S. 1 NRWPolG. Entsprechend: § 37 Abs. 2 S. 1 BWPolG; Art. 37 Abs. 2 S. 1 BayPAG; § 42 Abs. 2 S. 1 BerlASOG; § 38 Abs. 1 S. 1 BbgPolG; § 36a Abs. 1 S. 2 HBPolG; § 14 Abs. 1 S. 1 HHPolDVG; § 20 Abs. 2 HeSOG; § 38 Abs. 1 S. 1, 3 NdsSOG; § 33 Abs. 2 S. 1 RPPOG; § 30 Abs. 1 S. 2 SlPolG; § 43 Abs. 1 S. 2 SachsPolG; § 22 Abs. 2 S. 1 LSASOG; § 188 Abs. 1 S. 2 SHLVwG; § 39 S. 1 ThürPAG; § 36 Abs. 1 S. 2 MVSOG; § 29 Abs. 1 S. 3 BPolG.

[10] Dazu am Beispiel des Art. 10 GG plastisch BVerfGE 85, 386 (398 f.); *Gusy*, in: v. Mangoldt/Klein/Starck (Hrsg.), GG, 6. Aufl. 2011, Art. 10 Rn. 60.

[11] Dazu etwa § 24 Abs. 2 NRWPolG. Entsprechend: § 38 Abs. 1, 2 BWPolG; Art. 38 Abs. 2 BayPAG; § 42 Abs. 3 BerlASOG; § 39 Abs. 2 BbgPolG; § 36b Abs. 5 HBPolG; § 16 Abs. 2 HHPolDVG; § 20 Abs. 4 HeSOG; § 37 Abs. 1, 2 MVSOG; § 39 Abs. 3, 4 NdsSOG; § 33 Abs. 4 RPPOG; § 30 Abs. 2 SlPolG; § 43 Abs. 2 SachsPolG; § 23 LSASOG; § 189 Abs. 1 SHLVwG; § 40 Abs. 2 ThürPAG; § 29 Abs. 2 BPolG.

[12] Verarbeitungsverbot in § 16 Abs. 4 NRWPolG. Entsprechend: § 23 Abs. 2 BWPolG; Art. 34 Abs. 2 BayPAG; § 25 Abs. 4a BerlASOG; § 29 Abs. 6 BbgPolG; § 33 Abs. 4 HBPolG; § 27 Abs. 2 S. 2 HeSOG; § 34a Abs. 8 S. 5 MVSOG; § 33a Abs. 3 S. 1 NdsSOG; § 29 Abs. 3-5 RPPOG; § 28a Abs. 2, 5 S. 1 SlPolG; § 37 Abs. 5 S. 4 SachsPolG; § 186a Abs. 1-3 SHLVwG; § 5 Abs. 7, § 34b Abs. 1 S. 1, § 35 Abs. 2, 6, 7 ThürPAG.

[13] Dazu näher *Matheis*, Strafverfahrensänderungsgesetz 1999, 2006; s.a. *Bertram,* Die Verwendung präventiv-polizeilicher Erkenntnisse im Strafverfahren, 2009.

Veränderung durch die Behörden (§§ 483 ff. StPO),[14] ihre Nutzung in automatisierten Dateien (§ 490 StPO), Übermittlungsbefugnisse an andere Stellen (§§ 477 ff. StPO), Akteneinsichtsrechte der Justizbehörden gegenüber Dritten (§ 474 StPO) und Dritter gegenüber den Justizbehörden (§§ 475 f. StPO) sowie bestimmte Kontroll- und Rechtsschutzansprüche Betroffener (§§ 488 f. StPO).

b) Maßnahmen zur Abwehr von Gefahren richten sich nach den Polizeigesetzen des Bundes und der Länder. Sie enthalten sämtlich inzwischen auch die Aufgabe der Datenverarbeitung und besondere Regelungen zur Datenverarbeitung. Dazu zählen generalklauselartige Ermächtigungen zur Nutzung erhobener Daten, zur Errichtung von Dateien, besondere Regelungen über bestimmte Nutzungsformen, zur Informationserlangung von Dritten oder zur Weitergabe an Dritte, sowie einzelne Rechte Betroffener.

Die im Einzelnen nicht einfachen Regelungen[15] gehen von Folgendem aus: Datenverarbeitung durch die Polizei erfolgt nicht einfach zu polizeilichen Zwecken, sondern zum Zweck der Strafverfolgung oder dem davon zu unterscheidenden Zweck der Gefahrenabwehr. Werden also Informationen für den ersteren Zweck erhoben, so ist ihre Nutzung für letzteren ein Vorgang der Zweckänderung und damit ein Informationseingriff.[16] Maßgeblich für die anwendbare Rechtsgrundlage ist damit der Verwendungszweck: Werden Daten zu präventiven Zwecken erhoben, so richtet sich ihre Verwendung nach dem Polizeirecht. Werden sie hingegen zu repressiven Zwecken erhoben, so richtet sich ihre Verwendung nach den genannten Bestimmungen der StPO; sie richtet sich hingegen wieder nach Polizeirecht, soweit beide Datenmengen gemeinsam gespeichert und verarbeitet werden (§ 483 Abs. 2 StPO) oder aber soweit sie für präventive Zwecke weiterhin gespeichert oder verarbeitet werden sollen (§ 484 Abs. 4 StPO). Soweit die genannten Gesetze keine eigenständigen Regelungen enthalten, können subsidiär die Bestimmungen der Datenschutzgesetze von Bund und Ländern angewandt werden.

II. Formen der Informationsverarbeitung

Das Recht der polizeilichen Datenverarbeitung bezieht sich auf rechtmäßig erhobene Daten[17]; es ist aber sinngemäß auch auf sonstige polizeilich verarbeitete Daten anwendbar. Die Einzelregelungen legen entsprechend den allgemeinen Grundsätzen des Informationsverarbeitungsrechts (siehe etwa § 3 Abs. 4 BDSG) vier Verarbeitungsformen zugrunde: das Aufzeichnen bzw. Speichern von Informationen (dazu u. 1.), das Verändern von Informationen (dazu u. 2.), das Übermitteln von Informationen (dazu u. 3.) und das Löschen von Informationen (dazu u. 4.)

1. Aufzeichnen von Informationen

Ist eine Information zur Polizei gelangt, kann sie dort aufgezeichnet[18] oder gespeichert werden.[19] Hierunter versteht man deren Aufnahme oder Erfassung in einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.[20] Dies kann stattfinden durch Aufschreiben und Aufnahme in Akten, Sammlungen[21] oder Karteien, oder durch Speicherung in automatischen Datenverarbeitungsanlagen. Die Maßnahme verfolgt einen doppelten Zweck: Zunächst wird die Information bei der Behörde perpetuiert. Akten und Dateien vergessen nichts; sie sind das technisch institutionalisierte Gedächtnis der Behörde. Zudem wird die Information abrufbar und damit für den speichernden Mitarbeiter und andere verfügbar gemacht. Dadurch wird die Information für die spätere Polizeiarbeit und die gesamte Behörde nutzbar. Was diese Funktionen nicht erfüllt, ist keine Aufzeichnung oder Speicherung in dem genannten Sinne. Das gilt insbesondere für das bloße „Speichern" im Gedächtnis des Beamten, der sich später an die Information erinnern kann. Dies wird nicht als Akt der Datenspeicherung qualifiziert, da es hier an der Objektivierung und der Verfügbarmachung für die weitere Polizeiarbeit fehlt. Denn was nur einer weiß, kann kein anderer nutzen.

Die Aufzeichnung ist ein gegenüber der Erhebung selbständiger Akt.[22] Gespeichert werden können auch Daten, die freiwillig übermittelt, also nicht „erhoben" worden sind. Außerdem können alle Arten erlangter Informationen vor ihrer Speicherung ausgesondert werden oder im ausschließlichen Wissen des jeweiligen Mitarbeiters verbleiben, also eben nicht gespeichert werden. Der Eingriffsgehalt resultiert demnach aus dem Zusammentreffen zweier Umstände: dem Per-

[14] Dazu näher *Petri* (Fn. 7), H Rn. 385 ff.

[15] Gesamtüberblick bei *Petri* (Fn. 7), H Rn. 1 ff.

[16] Dazu § 481 StPO; ausgeführt in § 24 Abs. 2 S. 1 NRWPolG. Entsprechend: Art. 38 Abs. 2 S. 1 BayPAG; § 42 Abs. 3 BerlASOG; § 39 Abs. 2 S. 1, 2 BbgPolG; § 36b Abs. 5 S. 1 HBPolG; § 16 Abs. 2 S. 1 HHPolDVG; § 20 Abs. 4 HeSOG; § 37 Abs. 1 MVSOG; § 39 Abs. 3 S. 1 NdsSOG; § 33 Abs. 4 S. 1 RPPOG; § 30 Abs. 2 SlPolG; § 42 Abs. 2 S. 1 SachsPolG; § 23 LSASOG; § 189 Abs. 1 SHLVwG; § 40 Abs. 2 S. 1, 2 ThürPAG; § 29 Abs. 2 S. 1 BPolG.

[17] Zur polizeilichen Informationserhebung näher *Gusy* (Fn. 1), Rn. 201 ff.; *Schenke* (Fn. 1), Rn. 175 ff.; *Schoch* (Fn. 6), Kap. 2 Rn. 244 ff.

[18] §§ 22 ff. NRWPolG. Entsprechend: §§ 13 ff. BWLDSG; Art. 37 ff. BayPAG; §§ 42 ff. BerlASOG; §§ 37 ff. BbgPolG; § 36a HBPolG; §§ 14 ff. HHPolDVG; §§ 20 ff. HeSOG; §§ 36 ff. MVSOG; §§ 38 ff. NdsSOG; §§ 26 ff. RPPOG; §§ 30 ff. SlPolG; §§ 43 ff. SachsPolG; §§ 22 ff. LSASOG; §§ 188 ff. SHLVwG; §§ 38 ff. ThürPAG; §§ 29 ff. BPolG.

[19] § 24 Abs. 1 NRWPolG. Entsprechend: § 37 Abs. 1 S. 1 BWPolG; Art. 38 Abs. 1 BayPolG; § 42 Abs. 1 BerlASOG; § 39 Abs. 1 BbgPolG; § 36a Abs. 1 HBPolG; § 16 Abs. 1 HHPolDVG; § 20 Abs. 1 HeSOG; § 36 Abs. 1 S. 1 MVSOG; § 38 Abs. 1 NdsSOG; § 33 Abs. 1 RPPOG; § 30 Abs. 1 SlPolG; § 43 Abs. 1 SachsPolG; § 22 Abs. 1 LSASOG; § 188 Abs. 1 SHLVwG; § 40 Abs. 1 ThürPAG; § 29 Abs. 1 BPolG; § 24 Nr. 8 NRWOBG; § 23 Nr. 2d BbgOBG.

[20] *Dammann* (Fn. 7), § 3 Rn. 115.

[21] Zu solchen Sammlungen OVG Berlin NJW 1986, 2004; KG DVR 1982, 366.

[22] Gegen einen Grundsatz, wonach alle Daten, die erhoben werden dürfen, auch gespeichert werden dürfen, zu Recht *Petri* (Fn. 7), H Rn. 352; *Alberts*/*Merten*, HHDVPolG, 1995, § 16 Rn. 1.

sonenbezug der Information und ihrer Bereitstellung für die zukünftige Polizeiarbeit. Die Speicherung erzeugt einen Datenschatten der Betroffenen, mit dessen Inhalt sie „polizeilich bekannt" sind. Dieser Schatten tritt für die Zwecke der Polizeiarbeit regelmäßig an die Stelle der Person selbst: Wer als potentieller Gewalttäter gespeichert ist, läuft Gefahr, bei jedem Polizeikontakt als potentieller Gewalttäter behandelt zu werden, solange die Eintragung besteht. Das gilt auch dann, wenn er seine Einstellung oder sein Verhalten geändert hat, zumindest bis die Eintragung aktualisiert oder aufgehoben wird. Hierin liegt die wichtigste Eingriffswirkung gegenüber dem Betroffenen: „Seine" Daten werden entpersonalisiert; er selbst erscheint als bloße Ausprägung seiner Daten. Das gilt jedenfalls, solange die ihm gegenüber handelnden Beamten ihn – wie im Regelfall – nicht persönlich kennen. Erschwerend kommt außerdem hinzu, dass für Betroffene vielfach die Tatsache der Speicherung und deren Dauer nicht erkennbar sind. Mag die Einstellung in polizeiliche Informationssysteme für anwesende Betroffene noch erkennbar sein, so erfolgt doch deren weitere Speicherung bis zu ihrem Ende in ihrer Abwesenheit und daher stets unerkennbar. Hier müssen die gesetzlichen Regelungen einen schwierigen Spagat vollziehen: Einerseits sollen etwa gesuchte Verdächtige oder gefährliche Personen möglichst nicht erfahren was die Behörden wissen, um ihre Taten, ihren Aufenthaltsort oder ihre Pläne zu ermitteln. Andererseits sollen Unverdächtige oder Nichtverantwortliche, Zeugen, Anzeigeerstatter oder Opfer nicht mehr als nötig in polizeiliche Informationssysteme gelangen und so nicht mehr als nötig in ihrer Privatsphäre beeinträchtigt werden. Diesem ist durch die gesetzliche Ausgestaltung notwendiger Befugnisnormen einerseits und möglichst effektiver Befugnisgrenzen andererseits Rechnung zu tragen.

Im Grundsatz gilt: Polizeiliche Informationen dürfen zu polizeilichen Zwecken, also zum Schutz der öffentlichen Sicherheit – und ggf. öffentlichen Ordnung – sowie sonstiger geschützter Rechtsgüter[23] oder gesetzlich zugelassenen polizeilichen Zwecken[24] gespeichert werden.[25] Dieser Zweck muss im Speicherungszeitpunkt konkretisierbar sein; eine Datenverarbeitung zu unbestimmten Zwecken ist unzulässig.[26] Durften die Daten nur zu bestimmten Zwecken erhoben werden – etwa bei schwerwiegenden Grundrechtseingriffen –, so ist dieser Umstand mitzuspeichern, da solche Informationen nur zu vergleichbaren Zwecken verwendet werden dürfen und dies nachträglich für die verarbeitenden Stellen erkennbar sein muss (sog. Kennzeichnungspflicht).[27] Soweit der Speicherungszweck eine personenbezogene Aufbewahrung nicht (mehr) erfordert, sind die Daten zu anonymisieren. So entfallen der Personenbezug und damit der Grundrechtseingriff. Dies gilt etwa bei der Verarbeitung für statistische Zwecke, interne Dokumentationspflichten oder die Aus- und Fortbildung.[28] Die Grenzen der Speicherungsbefugnis folgen grundsätzlich dem allgemeinen Rechtsgedanken, wonach eine polizeiliche Maßnahme zu beenden oder aufzuheben ist, wenn ihr Zweck erreicht ist oder nicht mehr erreicht werden kann.[29] Doch hat sich diese Norm für den Bereich der Datenverarbeitung als relativ unpräzise erwiesen: Ob eine Information für die polizeiliche Aufgabenerfüllung in Zukunft (!) noch erforderlich[30] sein wird, ist ex ante schwer zu prognostizieren. Völlig ausgeschlossen erscheint dies nahezu niemals. Es bedarf daher einer Abwägung zwischen der möglicherweise verbleibenden Erforderlichkeitswahrscheinlichkeit einerseits und der Intensität des Grundrechtseingriffs andererseits.[31]

Bekanntester Beispielsfall ist die Aufbewahrung erkennungsdienstlicher Unterlagen, die gerade der Wiedererkennung des Betroffenen und damit zukünftiger Polizeiarbeit

[23] Zu den Schutzgütern des Polizeirechts *Gusy* (Fn. 1), Rn. 77 ff.; *Denninger*, in: Lisken/Denninger (Fn. 7), E Rn. 16 ff.; *Schenke* (Fn. 1), Rn. 53 ff.; *Schoch* (Fn. 6), Kap. 2 Rn. 8 ff., 20 ff.

[24] Zu diesen näher § 1 Abs. 1 S. 2, Abs. 5 S. 2 i.V.m. §§ 9 ff. NRWPolG.

[25] § 24 Abs. 1 NRWPolG. Entsprechend: § 37 Abs. 1 BWPolG; Art. 38 Abs. 1 BayPolG; § 42 Abs. 1 BerlASOG; § 39 Abs. 1 BbgPolG; § 36a Abs. 1 HBPolG; § 16 Abs. 1 HHPolDVG; § 20 Abs. 1 HeSOG; § 36 Abs. 1 S. 1 MVSOG; § 38 Abs. 1 NdsSOG; § 33 Abs. 1 RPPOG; § 30 Abs. 1 SlPolG; § 43 Abs. 1 SachsPolG; § 22 Abs. 1 LSASOG; § 188 Abs. 1 SHLVwG; § 40 Abs. 1 ThürPAG; § 29 Abs. 1 BPolG; § 24 NRWOBG; § 23 Nr. 2d BbgOBG.

[26] BVerfG NJW 2010, 833 (839).

[27] Dazu näher BVerfGE 100, 313 (360 f.); 110, 33 (70 f.).

[28] § 24 Abs. 7, 6 NRWPolG. Entsprechend: § 37 Abs. 4, 3 BWPolG; Art. 38 Abs. 5 BayPAG; § 42 Abs. 4 BerlASOG; § 39 Abs. 6, 7 BbgPolG; § 17 Abs. 1, 2 HHPolDVG; § 20 Abs. 7 HeSOG; § 36 Abs. 4 MVSOG; § 39 Abs. 7, § 38 Abs. 4 NdsSOG; § 33 Abs. 7 RPPOG; § 30 Abs. 6 SlPolG; § 43 Abs. 6 SachsPolG; § 25 Abs. 1 LSASOG; § 188 Abs. 4 SHLVwG; § 40 Abs. 4, 3 ThürPAG; § 29 Abs. 6 BPolG; § 24 Nr. 8 NRWOBG; § 23 Nr. 2d BbgOBG.

[29] § 2 Abs. 3 NRWPolG. Entsprechend: Art. 4 Abs. 3 BayPAG; § 8 Abs. 3 BayLStVG; § 11 Abs. 3 BerlASOG; § 3 Abs. 3 BbgPolG; § 3 Abs. 3 HBPolG; § 4 Abs. 3 HeSOG; § 15 Abs. 3 MVSOG; § 4 Abs. 3 NdsSOG; § 2 Abs. 3 RPPOG; § 2 Abs. 3 SlPolG; § 3 Abs. 3 SachsPolG; § 5 Abs. 3 LSASOG; § 4 Abs. 3 ThürPAG; § 15 Abs. 3 BPolG; § 15 Abs. 3 NRWOBG. Betroffene können aus dieser Norm einen Unterlassungs-, Beseitigungs- oder Aufhebungsanspruch herleiten; siehe dazu *Gusy* (Fn. 1), Rn. 397; *Albers*, in: Hoffmann-Riem u.a. (Fn. 2), § 22 Rn. 79 ff.; *Schenke* (Fn. 1), Rn. 218.

[30] So der Wortlaut des § 22 S. 2 NRWPolG. Entsprechend: § 38 Abs. 4 S. 1 BWPolG; Art. 37 Abs. 3 S. 2 BayPAG; § 48 Abs. 4 S. 1 BerlASOG; § 37 S. 2 BbgPolG; § 36k Abs. 4 S. 1 HBPolG; § 15 S. 2 HHPolDVG; § 27 Abs. 4 S. 1 HeSOG; § 46 S. 1, § 47 Abs. 1 S. 1 MVSOG; § 47 Abs. 1 S. 1 NdsSOG; § 33 Abs. 3 S. 2 RPPOG; § 38 Abs. 2 S. 1 Nr. 2 SlPolG; § 43 Abs. 3 S. 2 SachsPolG; § 32 Abs. 2 S. 1 Nr. 2 LSASOG; § 196 Abs. 2 S. 1 SHLVwG; § 38 S. 2 ThürPAG; § 35 Abs. 2 Nr. 2 BPolG; § 24 Nr. 7 NRWOBG; § 23 Nr. 2b BbgOBG.

[31] OVG Ms. DÖV 1999, 522; OVG Koblenz DÖV 2001, 212; BayVGH NVwZ-RR 1998, 496.

dienen sollen.[32] Hier besteht Einigkeit, dass die Unterlagen nicht aufbewahrt werden dürfen, wenn ihre Erhebung rechtswidrig war oder wenn sie nur der Identifikation des Betroffenen diente und dieser identifiziert ist.[33] Bei Maßnahmen zur Gefahrenabwehr ist die Speicherung unzulässig, wenn sie zur Verhütung zukünftiger Straftaten nichts beizutragen vermag, insbesondere bei Fahrlässigkeitstaten oder erstmaliger Begehung von Bagatellstraftaten.[34] Im Übrigen wird die (weitere) Speicherung unzulässig bei nachträglichem Fortfall der Umstände, welche zur erkennungsdienstlichen Behandlung Betroffener geführt haben. Dabei sind primär eindeutige und nachvollziehbare nachträgliche Veränderungen der Einstellung oder des Verhaltens des Betroffenen zugrunde zu legen. Hier ist demnach der Einzelfall maßgeblich. Es wird jedenfalls dann angenommen, wenn eine andauernde Gefahrprognose nicht mehr gestellt werden kann und deshalb ausgeschlossen werden könnte, dass die weitere Aufbewahrung der Daten für die polizeiliche Aufklärungsarbeit (noch) notwendig sein wird.[35] Ein solcher Fall liegt vor, wenn die ursprüngliche Gefahrenprognose widerlegt ist, wenn das zugrunde liegende Strafverfahren nach § 170 Abs. 2 StPO eingestellt oder wenn der Betroffene freigesprochen ist.[36] Bei Einstellung des Strafverfahrens bedarf es einer Abwägung: Zwar ist hier die weitere Speicherung nicht völlig ausgeschlossen. Doch ist ein geringer fortbestehender Verdachtsgrad, eine festgestellte Geringfügigkeit der Schuld oder ein nur geringer Schaden aus der Straftat indiziell für ein Überwiegen der Rechtsgüter des Betroffenen.[37] In jedem Falle ist auch eine Abwägung mit den Rechten der gespeicherten Personen notwendig.

Da die genannten Feststellungen im Einzelfall schwierig sein mögen – schließlich hören die „polizeilichen Zwecke" niemals auf –, sind sie in den Polizeigesetzen durch zwei Vorkehrungen konkretisiert.

- (1) Da sind zunächst bestimmte Speicherungshöchstfristen: Nach deren Ablauf sind die aufgezeichneten Informationen zu löschen, wenn nicht zwischenzeitlich neue Gründe für ihre Erhebung bzw. Speicherung eingetreten sind. Dies gilt etwa für Kontakt- oder Begleitpersonen Verantwortlicher,[38] für die Aufzeichnung von Notrufen[39] und Informationen über bestimmte Minderjährige.[40] Sind die Fristen abgelaufen, so sind die Daten regelmäßig zu löschen; auf die Löschung besteht ein Anspruch der Betroffenen.[41]
- (2) Da sind daneben Prüfungspflichten, nach deren Ablauf von Amts wegen die weitere inhaltliche Richtigkeit der Informationen und die Notwendigkeit ihrer fortdauernden Speicherung festzustellen ist. Sie begründen die verfahrensrechtliche Verpflichtung zur Überprüfung, nicht aber automatisch zur Löschung von Informationen.

Unrichtige Informationen sind zu berichtigen. Eine solche Berichtigungspflicht,[42] die einem Berichtigungsanspruch des

---

[32] Zum Erkennungsdienst als „Wiedererkennungsdienst" *Dreier*, JZ 1987, 1009; zu den Rechtsfragen der Aufbewahrung erhobener Unterlagen grundsätzlich *Gusy*, VerwArch 1993, 441.

[33] § 14 Abs. 2 NRWPolG. Entsprechend: § 36 Abs. 3 BWPolG; Art. 14 Abs. 2 BayPAG; § 23 Abs. 2 BerlASOG; § 13 Abs. 3 BbgPolG; § 11b Abs. 2 HBPolG; § 7 Abs. 2 HHPolDVG; § 19 Abs. 4 HeSOG; § 31 Abs. 3 MVSOG; § 15 Abs. 2 NdsSOG; § 11 Abs. 2 RPPOG; § 10 Abs. 2 SlPolG; § 20 Abs. 3 SachsPolG; § 21 Abs. 3 LSASOG; § 183 Abs. 3 SHLVwG; § 16 Abs. 2 ThürPAG; § 24 Abs. 2 BPolG.

[34] *Petri* (Fn. 7), H Rn. 364 m.w.N.

[35] So oder ähnlich BVerwG, Buchholz 402.41 Nr. 47, 56; NWVGH NJW 1987, 2763.

[36] § 24 Abs. 2 S. 5 NRWPolG. Entsprechend: § 38 Abs. 1 S. 4 BWPolG; Art. 38 Abs. 2 S. 2 BayPAG; § 42 Abs. 3 BerlASOG; § 39 Abs. 2 S. 5 BbgPolG; § 36b Abs. 5 HBPolG; § 16 Abs. 2 HHPolDVG; § 20 Abs. 4 S. 2 HeSOG; § 37 Abs. 2 S. 2 MVSOG; § 39 Abs. 3, 4, § 39a S. 1 NdsSOG; § 39 Abs. 2 Nr. 1 RPPOG; § 30 Abs. 3 S. 1, 3, § 38 Abs. 2 S. 1 SlPolG; § 43 Abs. 2 S. 2 SachsPolG; §§ 23, 32 Abs. 2 S. 1 LSASOG; § 189 Abs. 2 S. 3 SHLVwG; § 40 Abs. 2 S. 5 ThürPAG; § 29 Abs. 2 S. 4 BPolG. So wohl auch die Tendenz in BVerfG NJW 2001, 3231, z.T. weiter gehend aber die polizeiliche Praxis, s. etwa Landesdatenschutzbeauftragter Bbg, 10. Tätigkeitsbericht, 2002, S. 73 ff.

[37] *Petri* (Fn. 7), H Rn. 369; *Rachor*, in: Lisken/Denninger (Fn. 7), F Rn. 464 ff. (beide m.w.N.).

[38] § 24 Abs. 4 NRWPolG. Entsprechend: § 37 Abs. 1 BWPolG; § 43 Abs. 1 BerlASOG; § 39 Abs. 4 BbgPolG; § 16 Abs. 3 HHPolDVG; § 20 Abs. 5 HeSOG; § 39 Abs. 5 NdsSOG; § 33 Abs. 5 RPPOG; § 22 Abs. 4 LSASOG; § 189 Abs. 4 SHLVwG; § 29 Abs. 3 BPolG.

[39] § 24 Abs. 5 NRWPolG. Entsprechend: § 42 Abs. 1 S. 2 BerlASOG; § 39 Abs. 5 BbgPolG; § 36a Abs. 4 HBPolG; § 27 Abs. 4 MVSOG; § 38 Abs. 3 NdsSOG; § 30 RPPOG, § 23a LSASOG.

[40] § 22 S. 5 NRWPolG. Entsprechend: § 38 Abs. 4 S. 2, Abs. 5 BWPolG; Art. 38 Abs. 3 S. 3, 5 BayPAG; § 48 Abs. 4 S. 2, 3 BerlASOG; § 37 S. 5 BbgPolG; § 36k Abs. 4 S. 2, 3 HBPolG; § 15 S. 5 HHPolDVG; § 27 Abs. 4 S. 2, 3 HeSOG; § 46 S. 2, 3 MVSOG; § 47 Abs. 1 S. 2, 3 NdsSOG; § 33 Abs. 4 S. 2 RPPOG; § 38 Abs. 2 S. 2, 3 SlPolG; § 43 Abs. 4 S. 1, 3 SachsPolG; § 32 Abs. 4 S. 1, 2 LSASOG; § 196 Abs. 3 S. 1, 2 SHLVwG; § 38 S. 5 ThürPAG; § 35 Abs. 3 S. 2, 3 BPolG; § 24 Nr. 7 NRWOBG; § 23 Nr. 2b BbgOBG.

[41] § 32 Abs. 2 NRWPolG. Entsprechend: § 46 Abs. 1 BWPolG i.V.m. § 23 BWLDSG; Art. 45 Abs. 2, 3 BayPAG; § 48 Abs. 2, 3 BerlASOG; § 47 Abs. 2, 5 BbgPolG; § 36k Abs. 2, 3 HBPolG; § 24 Abs. 2 HHPolDVG; § 27 Abs. 2 HeSOG; § 45 Abs. 2 S. 1, Abs. 4 MVSOG; §§ 39a, 47 Abs. 3 S. 1 NdsSOG, § 17 Abs. 2, 3 NdsLDSG; § 39 Abs. 2, 3 RPPOG; § 38 Abs. 2, 4 SlPolG; § 49 SachsPolG i.V.m. § 20 f. SachsLDSG; § 32 Abs. 2, 3 LSASOG; § 196 Abs. 2, 5 SHLVwG; § 45 Abs. 2, 4 ThürPAG; § 35 Abs. 2, 6 BPolG; § 24 Nr. 12 NRWOBG; § 23 Nr. 2f BbgOBG.

[42] § 32 Abs. 1 NRWPolG. Entsprechend: § 46 Abs. 2 BWPolG i.V.m. § 22 Abs. 1 BWLDSG; Art. 45 Abs. 1 BayPAG; § 48 Abs. 1 BerlASOG; § 47 Abs. 1 BbgPolG; § 36k Abs. 1 HBPolG; § 24 Abs. 1 HHPolDVG; § 27 Abs. 1 HeSOG; § 45 Abs. 1, 2 S. 2 MVSOG; § 47 Abs. 3 S. 1 NdsSOG, § 17

Betroffenen entspricht,[43] bezweckt einerseits die Aktualitätspflege der Datenbestände – denn veraltete und unrichtige Informationen nutzen der Polizei nichts –, wie auch die Wahrung der Rechte Betroffener: Sie können aufgrund unrichtiger Daten mit Grundrechtseingriffen konfrontiert werden, welche bei deren Richtigkeit unterblieben wären. Die Verfahrenspflicht dient zugleich der regelmäßigen Kontrolle der Fortdauer einer Datenspeicherung: Da die Betroffenen regelmäßig von dieser Tastsache keine Kenntnis haben,[44] können sie auch keine Überprüfung oder Löschung verlangen oder gar gerichtlich durchsetzen. Insoweit ist die Statuierung von Prüfungspflichten ein bescheidenes Surrogat für den hier regelmäßig nicht effektiven Rechtsschutz. In der Praxis ist die regelmäßige Überprüfung jedoch sehr sinnvoll; insbesondere veraltete Bestände und „Datenfriedhöfe" können so beseitigt werden. Bei der Einrichtung besonderer Dateien sind hierzu wichtige prozedurale Regelungen statuiert. Deren Einrichtung ist auf das notwendige Maß zu beschränken; dabei sind regelmäßige Termine für die Prüfungspflichten und in bestimmten Fällen Speicherungshöchstdauern zu bestimmen.[45] In einzelnen Normen wird partiell zwischen suchfähiger und nicht-suchfähiger Speicherung unterschieden.[46] Suchfähig sind Daten, welche in Dateien gespeichert sind, die technisch[47] und rechtlich bzw. organisatorisch den nutzenden Behörden die Möglichkeit eröffnen, Dateiinhalte aufgrund bestimmter Suchwörter oder Suchkriterien zu nutzen. Nicht alle Dienststellen können und dürfen auf alle Dateien ganz und unmittelbar zurückgreifen. Dies scheint insbesondere bei von Zentralstellen gespeicherten Informationen der Fall zu sein, wenn diese den einzelnen Polizeidienststellen nicht stets und in vollem Umfang zugänglich geschaltet sind, sondern oft nur für bestimmte Nutzungsformen oder -zwecke geöffnet werden. Diese können dann Suchfähigkeit ermöglichen. Alle anderen Informationen sind (für sie) nicht-suchfähig.

Einen Begleiteingriff zur Speicherung kann der Datenabgleich[48] darstellen. Dadurch können anfallende Daten einer Person – etwa eines Verantwortlichen – mit den vorhandenen Datenbeständen der Polizei verglichen werden, um festzustellen, ob die Person bereits irgendwo gespeichert ist. Dadurch können Informationen aus dem Einzelfall mit vorhandenen polizeilichen Kenntnisständen ergänzt werden. Zugleich kann auf diese Weise geprüft werden, ob und ggf. wo weitere Daten zu der Person zu speichern sind. Wer etwa vor einem Fußballspiel angetrunken und grölend durch die Innenstadt zieht, kann etwa daraufhin überprüft werden, ob er als Hooligan bzw. Gewalttäter registriert ist. Zum Zweck dieser Überprüfung können die Betroffenen angehalten werden.[49]

2. Verändern von Informationen

Die Vorschriften[50] betreffen das inhaltliche Umgestalten von Daten, welches den Informationsgehalt verändern kann.[51] Dazu können formelle Änderungen (anderes Datum), die Änderungen des Informationskontextes (Einordnung in eine Rubrik, etwa: gefundene Gegenstände statt verlorene Gegenstände), wie auch die Zusammenführung mit anderen Informationen zählen. Aus einem Zusammenhang können weitere Informationen gewonnen werden. Aber auch der umgekehrte Vorgang, das Herauslösen von Informationen aus ihrem Zu-

Abs. 1 NdsLDSG; § 39 Abs. 1 RPPOG; § 38 Abs. 1 SlPolG; § 49 SachsPolG i.V.m. § 19 Abs. 1 SachsLDSG; § 196 Abs. 1 SHLVwG; § 45 Abs. 1 ThürPAG; § 35 Abs. 1 BPolG; § 24 Nr. 12 NRWOBG; § 23 Nr. 2f BbgOBG.

[43] Zu diesem näher unter III.

[44] Auskunftsansprüche gegen die Polizei bestehen schon wegen der notwendigen Geheimhaltung zahlreicher Informationen nur in ganz rudimentärem Umfang; siehe näher etwa § 18 Abs. 1, 3 NRWDSG. Entsprechend: § 18 Abs. 3, 4 HeDSG; § 13 Abs. 1, 7 ThürDSG; § 20 Abs. 1, 2 SlDSG; § 27 Abs. 1, 2 SHLDSG; § 24 Abs. 1, 3, 4 MVDSG; Art. 10 Abs. 1, 7 BayDSG; § 18 Abs. 1, 6 BbgDSG; § 16 Abs. 1, 4 BerlDSG; § 16 Abs. 1, 3, 6 NdsDSG; § 18 Abs. 1, 6 HHDSG; § 18 Abs. 1, 3 SachsDSG; § 15 Abs. 1, 6 LSADSG; § 21 Abs. 1 HBDSG; § 18 Abs. 3, 7 RPDSG.

[45] §§ 22, 33 NRWPolG. Entsprechend: § 38 Abs. 4, § 42 Abs. 3 BWPolG; Art. 37 Abs. 3, Art. 46 f. BayPAG; § 42 Abs. 1, §§ 46, 48 Abs. 4, § 49 BerlASOG; §§ 37, 48 f. BbgPolG; §§ 36e, 36k Abs. 4 HBPolG; §§ 15, 26 f. HHPolDVG; §§ 24, 27 Abs. 4, § 28 HeSOG; § 40 Abs. 3, §§ 42, 46 MVSOG; §§ 40, 42 Abs. 5, § 47 NdsSOG; § 33 Abs. 3, §§ 36, 41 RPPOG; §§ 35, 38 Abs. 2, § 39 SlPolG; § 43 Abs. 3, §§ 48, 50 SachsPolG; § 32 Abs. 4 LSASOG; § 192 Abs. 4, §§ 194, 196 Abs. 3, § 197 SHLVwG; §§ 38, 42, 46 ThürPAG; §§ 33 Abs. 7, 8, § 35 Abs. 3, § 36 BPolG; § 23 Nr. 2b, 2f BbgOBG; § 24 Nr. 7 NRWOBG.

[46] Zu dieser Unterscheidung *Tegtmeyer/Vahle*, PolG NRW, 10. Aufl. 2006, § 32 Rn. 6.

[47] Allein auf technische Fragen stellen ab *Berner/Köhler*, BayPAG, 20. Aufl. 2010, S. 555, wonach es „nach dem heutigen Stand der Technik kaum vorstellbar erscheint, dass es in Dateien auch nicht suchfähig gespeicherte Daten gibt."

[48] Dazu § 25 NRWPolG. Entsprechend: § 39 BWPolG; Art. 43 BayPAG; § 28 BerlASOG; § 40 BbgPolG; § 36h HBPolG; § 22 HHPolDVG; § 25 HeSOG; § 43 MVSOG; § 45 NdsSOG; § 37 RPPOG; § 36 SlPolG; § 46 SachsPolG; § 30 LSASOG; § 195 SHLVwG; § 43 ThürPAG; § 34 BPolG.

[49] § 25 Abs. 2 NRWPolG. Entsprechend: § 39 Abs. 1 S. 4 BWPolG; Art. 43 Abs. 1 S. 4 BayPAG; § 28 Abs. 1 S. 3 BerlASOG; § 40 Abs. 2 BbgPolG; § 22 Abs. 2 HHPolDVG; § 25 Abs. 1 S. 4 HeSOG; § 45 Abs. 2 NdsSOG; § 37 Abs. 2 S. 2 RPPOG; § 46 Abs. 1 S. 4 SachsPolG; § 30 Abs. 1 S. 4 LSASOG; § 43 Abs. 3 ThürPAG; § 34 Abs. 1 S. 3 BPolG. Zum Anhalterecht *Petri* (Fn. 7), H Rn. 493 ff.

[50] § 24 Abs. 1, 2, 4 NRWPolG. Entsprechend: § 37 Abs. 1, § 38 Abs. 1, 2 BWPolG; Art 38 Abs. 1, 2 BayPAG; § 42 Abs. 1, 3, § 43 Abs. 1 BerlASOG; § 39 Abs. 1, 2, 4 BbgPolG; § 36a Abs. 1, § 36b Abs. 5 HBPolG; § 16 Abs. 1, 2, 3 HHPolDVG; § 20 Abs. 1, 4, 5 HeSOG; § 36 Abs. 1, § 37 Abs. 1, 2 MVSOG; § 38 Abs. 1, § 39 Abs. 3-5 NdsSOG; § 33 Abs. 1, 4, 5 RPPOG; § 30 Abs. 1, 2 SlPolG; § 43 Abs. 1, 2 SachsPolG; § 22 Abs. 1, 4, § 23 LSASOG; § 188 Abs. 1, § 189 Abs. 1, 4 SHLVwG; § 40 Abs. 1, 2 ThürPAG; § 29 Abs. 1-3 BPolG; § 24 Nr. 8 NRWOBG; § 23 Nr. 2d BbgOBG.

[51] *Dammann* (Fn. 7), § 3 Rn. 129 ff.

sammenhang, ist eine Veränderung, welche dem gleichen Zweck dienen kann. Am Beispiel: Hat in der Innenstadt eine gewalttätige Versammlung stattgefunden (Information 1) und ist A an diesem Tag in die Innenstadt gereist (Information 2), so stellt die Zusammenführung (A hat an der gewalttätigen Versammlung in der Innenstadt teilgenommen) eine neue Information (Information 3) dar. Der daraus gezogene Schluss, wonach A als Gewalttäter in Betracht kommt (Information 4), stellt dann durch Herauslösen aus dem Zusammenhang eine weitere veränderte Information dar. Eine solche Veränderung im Einzelfall ist Grundlage polizeilicher Aufklärungsarbeit und Gefahrenabwehr. Sie findet sich bei zahlreichen Maßnahmen routinemäßig, etwa bei der erkennungsdienstlichen Behandlung.

Hauptfall der Veränderung von Informationen in der polizeilichen Informationsinfrastruktur ist die Einstellung von Daten in bestimmte Dateien,[52] z.B. als „Gefährliche Gewalttäter", „gewaltbereite Extremisten", Fahndungsdateien, DNA-Analysedateien, Erkennungsdienst u.ä. Durch sie werden die Einzeldaten in einen Kontext gestellt, welcher ihnen zugleich eine zusätzliche Bedeutung zuweist: Die entsprechende Person ist nicht nur bei einer Schlägerei angetroffen, sondern neigt häufiger zu Handgreiflichkeiten und ist daher stets suchfähig gespeichert und auffindbar, wenn nach potentiellen Gewalttätern gesucht wird. Dabei ist schon die Zuschreibung im Titel oder die Umschreibung des Dateiinhalts eine „Veränderung" der in ihr enthaltenen Einzeldaten; das kann auch für Änderungen von Bezeichnungen gelten.[53] Solche Dateien unterliegen deshalb besonderen Anforderungen mit dem Ziel der Begrenzung ihrer Anzahl, der Selbstkontrolle der errichtenden Behörden und ihrer Überwachung durch Aufsichtsbehörden und Datenschutzbeauftragte.[54]

Sie bedürfen daher:

- (1) einer besonderen Errichtungsanordnung.[55] Sie ergeht formlos mit Innenwirkung, unterliegt allerdings zumeist besonderen Verfahrens- oder Zuständigkeitsregelungen (z.B.: Errichtung nur durch den Innenminister). Wo das Gesetz die Errichtung durch Rechtsverordnung vorschreibt, ist diese die Zulässigkeitsbedingung für die Verarbeitung von Informationen in Dateien.[56] In Eilfällen dürfen zeitlich befristete Dateien auch ohne besondere Anordnung eingerichtet werden, nach Ablauf gesetzlich festgelegter Dauern muss der notwendige Verfahrensablauf nachgeholt werden. (z.B. § 41 Abs. 3 S. 3 RPPOG oder § 36 Abs. 2 S. 2 BPolG).
- (2) einer Prüfung der Erforderlichkeit, ob die notwendige technische Form der Dateien (in Akten oder elektronisch, suchfähig oder nichtsuchfähig) und die Notwendigkeit ihrer Dauer eingehalten sind. Die Errichtung ist zu befristen, die Notwendigkeit ihrer Weiterführung oder Änderung in angemessenen zeitlichen Abständen zu überprüfen.[57] Nicht nur die einzelnen Informationen, sondern auch jede polizeiliche Datei muss für den konkret angebbaren polizeilichen Zweck geeignet, erforderlich und verhältnismäßig sein.
- (3) der Angabe der maßgeblichen Rechtsgrundlage, des Zwecks der Datei, des Datenumfangs, der Zugriffsberechtigten, der Übermittlungsregelungen, der Speicher- bzw. Prüffristen und der zu ihrer Einhaltung zu ergreifenden technischen und organisatorischen Maßnahmen.[58]

Besonderen Anforderungen unterliegen gemeinsame Dateien unterschiedlicher Behörden, wenn ein Direktabruf möglich ist, oder länderübergreifende Dateien.[59] Im Übrigen gelten für die Veränderung die Vorschriften über die Datenspeicherung – soweit sie sinngemäß übertragbar sind – entsprechend. Daneben finden weitere Vorschriften der Datenschutzgesetze Anwendung.

3. Übermitteln von Informationen

a) Grundlagen

Die Vorschriften[60] ermächtigen zur Bekanntgabe von Daten einer Behörde an Dritte. Es kann geschehen durch Weiterga-

[52] Wichtige Dateien wie etwa PIOS, SPUDOK, INPOL beschreibt *Petri* (Fn. 7), H Rn. 60 ff.

[53] Zu den Anforderungen *Petri* (Fn. 7), H Rn. 383; *Dammann* (Fn. 7), § 3 Rn. 134 ff.

[54] BVerfGE 65, 1 (46); 67, 157 (178 ff.); *Petri* (Fn. 7), H Rn. 383, 372.

[55] Siehe § 490 StPO; § 33 Abs. 1 S. 1 NRWPolG. Entsprechend: § 48 BWPolG i.V.m. § 11 BWLDSG; Art. 47 BayPAG; § 49 BerlASOG; § 48 BbgPolG; § 36j HBPolG; §§ 26 f. HHPolDVG; § 28 HeSOG; § 47 Abs. 2 MVSOG; § 41 RPPOG; § 197 SHLVwG; § 39 SlPolG; § 50 SachsPolG; § 46 ThürPAG; § 36 BPolG.

[56] So etwa *Arzt*, NJW 2011, 352; OVG Lüneburg NdsVBl. 2009, 135; VG Wiesbaden NVwZ-RR 2011, 151; a.A. HeVGH NJW 2005, 2727 (2732); offen gelassen in BVerwG NJW 2011, 405.

[57] § 33 Abs. 1 S. 2 NRWPolG. Entsprechend: § 41 Abs. 1 BWPolG; Art. 47 Abs. 1, 2 BayPAG; § 49 Abs. 1, 3 BerlASOG; § 48 Abs. 1 BbgPolG; § 26 Abs. 3 S. 1 HHPolDVG; § 47 Abs. 1 MVSOG; § 46 Abs. 2 NdsSOG; § 41 Abs. 1 RPPOG; § 39 Abs. 1 SlPolG; § 50 SachsPolG; § 197 Abs. 1 SHLVwG; § 36 Abs. 3 BPolG.

[58] Dazu im Einzelnen §§ 22, 33 NRWPolG. Entsprechende Landesgesetze siehe oben Fn. 45.

[59] Etwa: § 33 Abs. 5, 6 NRWPolG. Entsprechend: § 42 Abs. 3, 4 BWPolG; Art. 46, 47 BayPAG; § 46 BerlASOG; § 49 BbgPolG; § 36e HBPolG; § 27 Abs. 1, 2 HHPolDVG; § 24 HeSOG; § 42 MVSOG; § 42 NdsSOG; § 36 RPPOG; § 35 SlPolG; § 48 SachsPolG; § 194 SHLVwG; § 42 ThürPAG; § 33 Abs. 7, 8 BPolG; s.a. §§ 4 ff. ATDG (BundesAntiterrordateiG v. 22.12.2006, BGBl. I 2006, S. 3409); dazu *Ellermann*, Polizei 2007, 181.

[60] §§ 26 ff. NRWPolG. Entsprechend: §§ 41 ff. BWPolG; Art. 39 ff. BayPAG; §§ 44 ff. BerlASOG; §§ 41 ff. BbgPolG; §§ 36c ff. HBPolG; §§ 18 ff. HHPolDVG; §§ 21 ff. HeSOG; §§ 39 ff. MVSOG; §§ 40 ff. NdsSOG; §§ 34 ff. RPPOG; §§ 32 ff. SlPolG; §§ 14 ff. SachsPolG; §§ 26 ff. LSASOG; §§ 191 ff. SHLVwG; §§ 41 ff. ThürPAG; §§ 32 ff. BPolG, §§ 24 Nr. 9 f. NRWOBG; § 23 Nr. 2e BbgOBG.

be der Informationen oder aber durch die Eröffnung der Einsichtnahme für die andere Stelle.[61] Die Übermittlung stellt regelmäßig einen Eingriff in den Zweckbindungsgrundsatz dar:[62] Durch sie werden Informationen, welche für den Zweck einer Stelle erhoben bzw. gespeichert worden sind, für andere Behörden und deren Zwecke nutzbar gemacht. Dabei wirkt der rechtlich mögliche Nutzungszweck zugleich auf den Erhebungsvorgang zurück: Je intensiver eine gesetzlich zugelassene Datennutzung in die Grundrechte Betroffener eingreifen kann, desto schwerer wiegt schon der vorgelagerte Grundrechtseingriff durch die Datenerhebung.[63] Umgekehrt wirkt der Erhebungseingriff weniger schwer, wenn die rechtlich mögliche Informationsverwendung eingegrenzt und auf geringere Eingriffe begrenzt ist. Das Polizeirecht regelt unterschiedliche Wege der Informationsübermittlung: den Austausch zwischen unterschiedlichen Polizeibehörden,[64] wobei der Datenaustausch mit ausländischen Polizeien regelmäßig höheren Anforderungen unterliegt;[65] eine Weitergabe liegt auch vor, wenn die Daten bei zentralen Polizeibehörden (etwa: BKA, LKA) gespeichert werden und anderen Polizeistellen zum Abruf offenstehen;[66] außerdem denjenigen zwischen Polizei und anderen staatlichen Stellen, wobei die Gesetze zwischen der Datenübermittlung durch die Polizei an andere Behörden[67] und durch andere Behörden an die Polizei[68] unterscheiden. Hier können ergänzend auch andere Gesetze, etwa über die Nachrichtendienste, einschlägig sein.[69] Sonderformen sind die Öffnung polizeilicher Daten für einen direkten Datenabruf durch andere Stellen und die Einstellung von Daten in gemeinsame Dateien mit anderen Stellen.[70] Auch hier unterliegt der Austausch mit ausländischen Stellen besonderen Einschränkungen;[71] schließlich den Austausch zwischen Polizei und Privaten.[72] Außerhalb dieser Befugnisnormen ist er unzulässig und kann eine Straftat nach § 353b Abs. 1 Nr. 1 StGB darstellen.

Die einschlägigen Gesetze kombinieren für die unterschiedlichen Übermittlungsformen und -adressaten regelmäßig vier Tatbestandsmerkmale miteinander:

- (1) Die Rechtfertigung der Übermittlung durch einen Behördenzweck: Dies kann der Zweck der übermittelnden Behörde (etwa: eine Stelle übermittelt Informationen über eine gesuchte Person mit der Bitte, diese in ihrem Zuständigkeitsbereich aufzuspüren) oder derjenigen Stelle sein, an welche die Informationen übermittelt werden (etwa: eine Verfassungsschutzbehörde ist auf eine drohende Straftat aufmerksam geworden und übermittelt sie an die Polizei mit dem Anliegen, diese Straftat möglichst zu verhindern).[73]
- (2) Die Erforderlichkeit der Übermittlung zur Wahrnehmung jenes Zwecks. Diese Ausprägung des Übermaßverbotes untersagt die Übermittlung, wenn der konkrete Zweck auch ohne sie erfüllt werden kann.
- (3) Das Fehlen entgegenstehender vorrangiger Rechtsgüter Betroffener: Greift die Übermittlung allein in das Grundrecht der informationellen Selbstbestimmung ein, so ist der Eingriff eher zu rechtfertigen als für den Fall, dass die Information in den Kernbereich privater Lebens-

[61] *Dammann* (Fn. 7), § 3 Rn. 143.
[62] Dazu oben I. 2.
[63] BVerfGE 115, 320 – Rasterfahndung.
[64] § 27 NRWPolG. Entsprechend: § 42 BWPolG; Art. 40 BayPAG; § 44 BerlASOG; § 42 BbgPolG; § 36d HBPolG; § 19 HHPolDVG; § 22 HeSOG; § 40 MVSOG; § 41 NdsSOG; § 34 RPPOG; § 33 SlPolG; § 14 SachsDSG; § 27 LSASOG; § 192 SHLVwG; § 41 Abs. 1 ThürPAG; § 32 Abs. 1 BPolG; § 24 Nr. 10 NRWOBG; § 23 Nr. 2e BbgOBG.
[65] Siehe etwa § 27 Abs. 2 NRWPolG. Entsprechend: § 43 Abs. 3 BWPolG; Art. 40 Abs. 5 BayPAG; § 44 Abs. 3 BerlASOG; § 42 Abs. 2 BbgPolG; § 36f Abs. 2 HBPolG; § 19 Abs. 2 HHPolDVG; § 22 Abs. 3 HeSOG; § 40 Abs. 4 MVSOG; § 43 Abs. 2, 4, 5 NdsSOG; § 34 RPPOG; § 33 Abs. 2 SlPolG; § 14 SachsDSG; § 27 Abs. 3 LSASOG; § 192 SHLVwG; § 41 Abs. 4 ThürPAG; § 32 Abs. 3 BPolG. Siehe dazu etwa BVerfG NVwZ 2005, 681 ff. Für das BKA gibt es keine Ermächtigungsgrundlage zur Informationsübermittlung an die NATO, VG Wiesbaden NVwZ-RR 2011, 151.
[66] § 33 NRWPolG. Entsprechend: § 42 Abs. 3, 4 BWPolG; Art. 46, 47 BayPAG; § 46 BerlASOG; § 49 BbgPolG; § 36e HBPolG; §§ 26, 27 HHPolDVG; § 24 HeSOG; § 42 MVSOG; § 42 NdsSOG; § 36 RPPOG; § 35 SlPolG; § 48 SachsPolG; § 194 SHLVwG; § 42 ThürPAG; § 33 Abs. 7, 8 BPolG.
[67] Dazu § 28 NRWPolG. Entsprechend: § 43 BWPolG; Art. 40 Abs. 2-5 BayPolG; § 44 Abs. 2, 3 BerlASOG; § 43 BbgPolG; § 36f HBPolG; § 20 HHPolDVG; § 22 Abs. 2-4 HeSOG; § 41 MVSOG; § 43 NdsSOG; § 34 Abs. 2-4 RPPOG; § 34 SlPolG; § 14 SachsDSG; § 27 Abs. 2-4 LSASOG; § 193 SHLVwG; § 41 Abs. 2-5 ThürPAG; § 32 Abs. 2, 3 BPolG; § 24 Nr. 11 NRWOBG; § 23 Nr. 2e BbgOBG.
[68] Dazu § 30 NRWPolG. Entsprechend: Art. 42 BayPAG; § 44 Abs. 7 BerlASOG; § 45 BbgPolG; § 36d Abs. 1 S. 2 HBPolG; § 41 NdsSOG; § 34 Abs. 6 RPPOG; § 27 Abs. 5 LSASOG; § 41 Abs. 7 ThürPAG; § 24 Nr. 11 NRWOBG.
[69] Siehe etwa §§ 18 ff. BVerfSchG; 8 f. BNDG.
[70] Zu unterschiedlichen Fallgestaltungen *Petri* (Fn. 7), H Rn. 466 ff.
[71] § 30 Abs. 3 NRWPolG. Entsprechend: Art. 42 Abs. 3 BayPAG; § 45 Abs. 3 BbgPolG; § 34 Abs. 6 RPPOG; § 27 Abs. 5 LSASOG; § 41 Abs. 7 ThürPAG.
[72] Dazu § 29 NRWPolG. Entsprechend: § 44 BWPolG; Art. 41 BayPAG; § 45 BerlASOG; § 44 BbgPolG; § 36g HBPolG; § 21 HHPolDVG; § 23 HeSOG; § 41 MVSOG; § 44 NdsSOG; § 34 Abs. 4, 5 RPPOG; § 34 SlPolG; § 45 SachsPolG; § 28 LSASOG; § 193 Abs. 1 SHLVwG; § 41 Abs. 3 S. 2 ThürPAG; § 32 Abs. 4 BPolG; § 24 Nr. 11 NRWOBG; § 23 Nr. 2e BbgOBG.
[73] Zum hier möglicherweise relevanten „Trennungsgebot" BVerfGE 97, 198 (217); dazu *Gusy*, in: Möllers/van Ooyen (Hrsg.), JBÖS 2008/2009, 2009, S. 177 ff.; *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaften und Nachrichtendiensten, 2002, S. 311 ff.; kritisch *König*, Trennung und Zusammenarbeit von Polizei und Nachrichtendiensten, 2005, S. 151 ff.

gestaltung,[74] die Intimsphäre, ein besonders geschütztes Amts-,[75] Berufs- oder Geschäftsgeheimnis[76] oder ein grundgesetzlich geschütztes Vertrauensverhältnis, welches etwa zur Zeugnisverweigerung vor Gericht berechtigen würde, eingreift.[77] Für solche Fälle und dann, wenn die Informationserhebung durch schwerwiegende Eingriffe in besonders geschützte Garantien, etwa Art. 13, 10, 6 GG eingreift, verlangt das BVerfG besondere gesetzliche Regelungen, welche die formellen und materiellen Übermittlungsvoraussetzungen und -grenzen näher umreißen.[78]

- (4) Keine Sperrung der Informationen: Gesperrte Informationen dürfen nicht übermittelt werden.[79] Dasselbe gilt für rechtswidrig erhobene oder gespeicherte Daten.[80]

Stellt sich im Nachhinein heraus, dass eine Information unzutreffend war oder nicht hätte übermittelt werden dürfen, so entsteht von Amts wegen eine Nachberichtspflicht, welche die falsche Information berichtigt oder auf die Unzulässigkeit der Übermittlung hinweist.

Wer Informationen erhält, darf sie grundsätzlich nur zu denjenigen Zwecken nutzen, zu denen sie ihm übermittelt worden sind. Dieser Zweckbindungsgrundsatz untersagt nachträgliche Zweckänderung. Sie wären eine Veränderung der Information und damit ihrerseits gesetzlich rechtfertigungsbedürftig.[81] Dies ist namentlich bei ausländischen Stellen und bei Privatpersonen schwer zu überprüfen, wenn ihre Datennutzung zugleich Teil der eigenen Grundrechtsausübung ist. Deshalb sind hier regelmäßig besondere Vorkehrungen nötig.

b) Fallgruppen

Einen Sonderfall behördlicher Datenweitergabe und -zusammenführung stellt die Fahndung dar. Die explizit lediglich in §§ 131 ff. StPO geregelte Maßnahme (dort „Ausschreibung" genannt) kann darauf gerichtet sein, unbekannte Verdächtige, gefährliche Personen oder Zeugen zu finden oder aber den unbekannten Aufenthalt einer bekannten Person zu erfahren. Intensivster Grundrechtseingriff ist dabei die Aufnahme einer Person in die Fahndungsdatei.[82] Deren rechtlich mögliches Ziel kann die Festnahme, Verhaftung oder Ingewahrsamnahme einer Person, ihre Aufenthaltsermittlung,[83] Abschiebung oder Zurückweisung an der Grenze sein. Dazu werden Angaben hinsichtlich des gesuchten Betroffenen[84] in besonderen polizeilichen Dateien zusammengeführt und diese sodann mit den Daten anderswo angetroffener Personen abgeglichen.[85] Der intensive Datenaustausch umfasst also neben der Speicherung zugleich die inner- und zwischenbehördliche Informationsweitergabe, ggf. die Möglichkeit zum Informationsabruf und den Abgleich von Informationen. Dabei richtet sich die Zulässigkeit der jeweiligen Einzelakte nach den hier dargestellten, jeweils für sie geltenden Regelungen der Polizeigesetze bzw. des Strafprozessrechts. Der Datenabgleich im Einzelfall, also der Vergleich der Daten der gesuchten mit denjenigen einer angetroffenen Person oder Sache, kann dann bei einem zufälligen Antreffen mutmaßlicher Gesuchter oder aber bei besonders eingerichteten Kontrollen (Kontrollstellen,[86] Grenzen u.a.) stattfinden.

---

[74] Siehe etwa § 16 NRWPolG. Entsprechend: § 23 Abs. 2, 5 BWPolG; Art. 34 Abs. 2, 5, Art. 34c Abs. 6 BayPAG; § 25 Abs. 4a BerlASOG; § 29 Abs. 6 BbgPolG; § 33 Abs. 4 HBPolG; § 27 Abs. 2 S. 2 HeSOG; § 34a Abs. 8, § 34b Abs. 2, 3 MVSOG; § 33a Abs. 3, § 35 Abs. 2, § 35a Abs. 2, 3, § 36a Abs. 5 NdsSOG; § 29 Abs. 3-5 RPPOG; § 28 Abs. 2, 5 SlPolG; § 186a Abs. 1-3 SHLVwG; § 5 Abs. 7, § 34b Abs. 1, 2, § 35 Abs. 2, 6, 7 ThürPAG; dazu grundlegend BVerfGE 109, 279 (314 ff.).

[75] Solche Geheimhaltungspflichten finden sich (mit Ausnahmen) etwa in §§ 5 PostG, 88 TKG, 35 SGB I, 67 ff. SGB X, 30 ff. AO.

[76] Dazu § 26 Abs. 2 NRWPolG. Entsprechend: § 41 Abs. 2 S. 2 BWPolG; Art. 39 Abs. 3 S. 1 BayPAG; § 44 Abs. 3 S. 2 BerlASOG; § 41 Abs. 2 BbgPolG; § 36c Abs. 1 S. 1, § 36b Abs. 3 HBPolG; § 18 Abs. 3 HHPolDVG; § 26 Abs. 1 S. 2, § 21 Abs. 2 HeSOG; § 39 Abs. 2 MVSOG; § 35 Abs. 4 RPPOG; § 32 Abs. 3 SlPolG; § 14 Abs. 3 S. 3 SachsDSG; § 26 Abs. 2 LSASOG; § 191 Abs. 2 SHLVwG; § 41 Abs. 6 ThürPAG; zum Geheimnisschutz im Polizeirecht etwa *Würtenberger/Schenke*, JZ 1999, 548.

[77] Dazu § 16 Abs. 5 NRWPolG. Entsprechend: Art. 34d Abs. 1 S. 4, 5 BayPAG; § 25 Abs. 4a BerlASOG; § 33a Abs. 5 BbgPolG; § 33 Abs. 9 HBPolG; § 27 Abs. 2 S. 2 HeSOG; § 34b Abs. 4, § 33 Abs. 6 MVSOG; § 35a Abs. 1 S. 3 NdsSOG; § 29 Abs. 6 RPPOG; § 28a Abs. 2 SlPolG; § 186a Abs. 4 SHLVwG; § 35 Abs. 2 ThürPAG.

[78] Etwa: BVerfGE 100, 313 (360 ff.).

[79] Zur Sperrung siehe unten II. 4.

[80] § 32 Abs. 4 NRWPolG. Entsprechend: § 48 Abs. 5 BerlASOG; § 47 Abs. 4 BbgPolG; § 24 Abs. 5 HHPolDVG; § 27 Abs. 5 HeSOG; § 45 Abs. 6 MVSOG; § 17 Abs. 4 NdsLDSG; § 38 Abs. 3 SlPolG; §§ 49 SachsPolG i.V.m. 19 Abs. 2 SachsLDSG; § 45 Abs. 3 ThürPAG; § 35 Abs. 8 BPolG; siehe etwa BayVGH NJW 1982, 2235; BWVGH NJW 1987, 3022.

[81] Dazu oben II. 2.

[82] Dazu *Schultheis,* in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 131 Rn. 9, § 131a Rn. 6; *Pfeiffer*, StPO, 5. Aufl. 2005, § 131 Rn. 2; *Frister*, in: Lisken/Denninger (Fn. 7), G Rn. 179 ff.

[83] Zu ihr § 131a StPO; näher *Schultheis* (Fn. 82), § 131a Rn. 2; *Pfeiffer* (Fn. 82), § 131a Rn. 2; *Paeffgen*, in: Wolter (Hrsg.), SK-StPO II, 4. Aufl. 2010, § 131a Rn. 2.

[84] Daneben kann es auch Ausschreibungen zur polizeilichen Beobachtung – dazu § 21 NRWPolG; entsprechend: Art. 36 BayPAG; § 27 BerlASOG; § 36 BbgPolG; § 31 HBPolG; § 13 HHPolDVG; § 17 HeSOG; § 35 MVSOG; § 37 NdsSOG; § 32 RPPOG; § 29 SlPolG; § 42 SachsPolG; § 19 LSASOG; § 187 SHLVwG; § 37 ThürSOG; § 31 BPolG – und zu Sachfahndungen nach gesuchten Sachen, etwa gestohlenen Pkws, geben.

[85] Beschrieben bei *Petri* (Fn. 7), H Rn. 74 ff., 82 ff.

[86] Diese sind in speziellen Polizeigesetzen zugelassen, siehe § 26 Abs. 1 Nr. 6 BWPolG; Art. 13 Abs. 1 Nr. 5 BayPAG; § 27a MVSOG; § 12 Abs. 6 NdsSOG; § 14 Abs. 1 Nr. 5 ThürPAG; § 23 Abs. 2 Nr. 3 BPolG; zu den Kontrollstellen

Eine praktisch äußerst seltene, rechtlich aber viel diskutierte Sonderform der lageabhängigen Aufklärungsbefugnisse ist die Rasterfahndung.[87] Dieser „Verdachts- bzw. Verdächtigengewinnungseingriff“[88] besteht darin, dass die Polizei eine Vielzahl behördlich gespeicherter Daten über Personen miteinander abgleicht, um auf diese Weise nach einem zuvor festgelegtem Raster diejenigen Datensätze herauszufiltern, deren Träger entweder eine Gefahr begründen oder als Verantwortliche für eine Gefahr in Betracht kommen können.[89] Die aus der Strafverfolgung stammende Maßnahme kombiniert also Merkmale wie etwa „alleinstehend“, „Mieter in einem großen Wohnblock“, „überdurchschnittliche Frequenz von Umzügen“, „Vorauszahler von Strom- und Wasserrechnungen in bar“, „polizeilich nicht gemeldet“, „kein Kfz“ und „kein Beitragszahler der Rentenversicherung“, um auf diese Weise mögliche Hinweise auf von Terroristen genutzte Wohnungen zu bekommen.[90] Die Maßnahme ist ihrer Konzeption nach notwendig ein Breitbandeingriff. Sie richtet sich gegen jeden, der Träger der im Raster enthaltenen Merkmale ist; also von vornherein fast ausschließlich gegen unverdächtige Personen. Ob überhaupt potentielle Gefährder innerhalb der Reichweite des Rasters liegen, ist zu diesem Zeitpunkt noch offen. Und selbst am Ende der Abgleiche kann dies bedeuten: Werden nach einem großen Abgleich nur 100 Personen überprüft, um zwei potentielle Gefährder zu ermitteln, so besteht für jede Einzelmaßnahme selbst nach Abschluss der Abgleiche höchstens eine Trefferwahrscheinlichkeit von 1: 49. Am Ende bleibt also eine mehr oder weniger große Zahl von Personen übrig, hinsichtlich derer „tatsächliche Anhaltspunkte“ für eine Gefahr oder Gefahrverursachung angenommen werden, welche mit besonderen Mitteln der Gefahraufklärung überprüft werden können. Nach der neueren Rechtsprechung[91] liegt ein Grundrechtseingriff nicht vor, soweit die Daten einzelner Personen automatisch erfasst, abgeglichen und spurenfrei wieder beseitigt werden, ohne dass eine Person sie zur Kenntnis nehmen oder die Daten später abrufen kann. Dies bedeutet insbesondere für die sog. „negative Rasterfahndung“: Wird nur danach gesucht, ob eine Person bestimmte Merkmale nicht erfüllt (z.B. „kein Mitglied der Rentenversicherung“), stellt die elektronische Aussonderung von Personen regelmäßig keinen Eingriff dar. Bei der „positiven“ Rasterfahndung, welche nach den Trägern bestimmter Merkmale sucht („Barzahler bei den Stadtwerken“), sind zumindest die Treffer als Eingriffe zu qualifizieren. Schwer wirkt hier schon die Summe der Abgleiche, welche bis zur Erstellung von Persönlichkeits- oder Bewegungsprofilen reichen können. Sie wirken auch deshalb schwer, da sie zu weiteren schwerwiegenden Eingriffen (wie etwa Befragungen, Recherchen in der Nachbarschaft, Observationen oder gar Durchsuchungen) bei gleichzeitig (extrem) geringem Wahrscheinlichkeitsgrad eines Aufklärungserfolges im Einzelfall führen können.[92] Solche überaus aufwändigen Methoden sind nach den meisten Polizeigesetzen[93] zulässig

- (1) entweder zum Schutz hochwertiger Rechtsgüter (Leben, Gesundheit, Freiheit einer Person) oder zur Verhinderung bestimmter Formen schwerer Kriminalität, also zur Abwehr schwerer Straftaten.
- (2) Dabei muss im Einzelfall eine zumindest konkrete Gefahr bestehen, im „Vorfeld“ einer Gefährdung darf die Maßnahme nicht durchgeführt werden.
- (3) Außerdem bedarf es der Einhaltung verfahrensrechtlicher Vorschriften wie dem Richtervorbehalt bzw. besonderer Behördenleitervorbehalte bis hin zum Innenminister. Speicherung und Verwendung von Informationen müssen darüber hinaus hinreichend bestimmt und verhältnismäßig geregelt werden.

Und dennoch bleibt die Eignung der Maßnahme für präventiv-polizeiliche Zwecke[94] sehr umstritten:[95] Ist noch kein Schaden eingetreten, ist die Erstellung eines Rasters noch schwieriger als nach begangenen Straftaten. So wurde nach dem 11.9.2001 kein einziger gesuchter „Schläfer“ entdeckt. „Erfolge“ der Maßnahmen stellten sich am ehesten durch Verunsicherung einzelner Szenen und die Ausreise bestimmter Personen ein. Dominierend war hier die symbolische Wirkung der Maßnahmen, welche für sich aber keine Grundrechtseingriffe rechtfertigt.

Einen weiteren Sonderfall stellt die Öffentlichkeitsfahndung (klassisch: Steckbrief) dar.[96] Fanden bei den zuvor ge-

grundlegend *Graf*, Verdachts- und ereignisunabhängige Personenkontrolle, 2006; *Krane*, „Schleierfahndung“, 2003.

[87] Zu ihr näher BVerfGE 115, 320 (367 ff.); OLG Düsseldorf NVwZ 2002, 629 (631); OLG Frankfurt NVwZ 2002, 626 (627); *Gusy*, KritV 2002, 474; *Volkmann,* JZ 2006, 918; *Schewe*, NVwZ 2007, 174; *Zschoch*, Die präventiv-polizeiliche Rasterfahndung, 2007; *Pohl*, Die Implementation der Rasterfahndung, 2008.

[88] Terminologie nach BVerfGE 115, 320 (355 ff.).

[89] Einzeldarstellung bei *Gusy*, KritV 2002, 474.

[90] Darstellung bei *Siebrecht*, Rasterfahndung, 1997, S. 52 f.

[91] BVerfGE 107, 299 (328); 115, 320 (343); 120, 378 (397 ff.).

[92] Zur erfolgsträchtigeren „kleinen Rasterfahndung“ durch freiwillige DNA-Reihenuntersuchung nach § 81h StPO s. BVerfG NJW 1996, 1587, 3071; BGH NStZ 2004, 392; *Gusy*, JZ 1996, 1176.

[93] § 31 NRWPolG; §§ 98a ff. StPO. Entsprechend: § 40 BWPolG; Art. 44 BayPAG; § 47 BerlASOG; § 46 BbgPolG, § 36i HBPolG; § 23 HHPolDVG; § 26 HeSOG; § 44 MVSOG; § 45a NdsSOG; § 38 RPPOG; § 37 SlPolG; § 47 SachsPolG; § 31 LSASOG; § 195 SHLVwG; § 44 ThürPAG; § 34 BPolG.

[94] Vgl. demgegenüber zur sog. „kleinen Rasterfahndung“ nach § 100g StPO: BVerfG NJW 2010, 833.

[95] Eher skeptisch *Gusy*, KritV 2002, 474; *Volkmann*, JZ 2006, 918; anders wohl *Geis/Möller*, Die Verwaltung 2004, 431; *Horn*, DÖV 2003, 746.

[96] Dazu § 131 Abs. 3, § 131a Abs. 3 StPO, näher *Schultheis* (Fn. 82), § 131 Rn. 14 ff., § 131a Rn. 4; *Pfeiffer* (Fn. 82), § 131 Rn. 4, § 131a Rn. 4; *Paeffgen* (Fn. 83), § 131 Rn. 6 f., § 131a Rn. 7 f.; OLG Hamm StV 1993, S. 4; *Soiné*, JR 2002, 137; *ders.*, NStZ 1997, 166 u. 321; *Pätzel*, NJW 1997, 3131; *Bär*, CR 1997, 422.

nannten Formen der Fahndung Informationsübermittlungen ausschließlich innerhalb der öffentlichen Verwaltung statt, so zeigt sich hier eine Datenweitergabe an jedermann, also auch an Private. Diese weitestgehende Form der Entprivatisierung personenbezogener Informationen[97] ist nur zulässig, wenn die gesetzlich umschriebenen Interessen der Strafverfolgung oder die öffentliche Sicherheit die Belange des Betroffenen erheblich überwiegen.[98] Die Veröffentlichung von Phantomzeichnungen kann nicht nur den Gesuchten, sondern auch dritte Personen, die dem Bild ähnlich sehen, tangieren.

4. Löschen von Informationen

Durch die Löschung[99] von Informationen werden diese unkenntlich gemacht, indem verhindert wird, dass aus gespeicherten Daten (noch) eine Information gewonnen werden kann.[100] Sie ist das Gegenstück zur Speicherung; der Speicherungsakt wird durch das Löschen aufgehoben. Fortan stehen die Informationen für die weitere Polizeiarbeit nicht mehr zur Verfügung; ihre Perpetuierung ist beendet; auch können sie Dritten nicht mehr bekannt gegeben werden.[101] Dessen ungeachtet können gelöschte Daten mit technischen Mitteln rekonstruierbar sein. Das „Löschen ohne Spuren“ wird demgegenüber als Vernichtung bezeichnet. Dadurch soll vermieden werden, dass durch die Art der Löschung (z.B. Übermalen mit Tipp-Ex), durch entstehende Aufzeichnungslücken oder durch die Möglichkeit der Rekonstruktion gelöschter Daten, Informationen wieder hergestellt werden können. Ein Minus gegenüber der Löschung ist die Sperrung von Daten, welche eine Information in besonderer Weise kennzeichnet, so dass deren Einsehbarkeit oder Abrufbarkeit durch einzelne (nicht alle) Berechtigte erschwert oder verhindert wird.[102]

Die Löschung kann nur durch die datenverwaltenden Stellen und insbesondere nahezu allein auf ihre Initiative stattfinden. Denn letztlich wissen nur sie, welche Daten an welcher Stelle noch vorhanden sind. Daher entstehen für sie Löschungspflichten, wenn[103]

- (1) die Datenspeicherung nicht (mehr) zulässig ist, also entweder von Anfang an unzulässig war oder aber nachträglich unzulässig geworden ist. Dies ist der Fall, wenn die Information rechtswidrig erlangt worden ist oder aber zur Erfüllung einer polizeilichen Aufgabe nicht mehr benötigt wird.[104] Dasselbe gilt, wenn eine gesetzliche oder durch Errichtungsanordnung festgesetzte Speicherungshöchstfrist abgelaufen ist[105] oder wenn bei periodischen Überprüfungen oder aus sonstigen Anlässen festgestellt wird, dass die Informationen nicht mehr benötigt werden.
- (2) die Löschung durch eine gesetzliche Spezialregelung bestimmt wird. Dies können Regelungen innerhalb der einzelnen Polizeigesetze sein, z.B. solche zum Schutz des unantastbaren Kernbereichs privater Lebensgestaltung[106] oder zur Durchsetzung von Richtervorbehalten[107] oder zum Schutz von Außenstehenden, welche von polizeilichen Fahndungsaktivitäten mitbetroffen sind.[108] Soweit anwendbar können allerdings auch andere gesetzliche Löschungsgebote in Betracht kommen, etwa § 489 StPO.

Derartige Löschungspflichten gelten regelmäßig nur für suchfähig gespeicherte personenbezogene Informationen. Nur sie können insbesondere regelmäßig auf ihre weitere Notwendigkeit überprüft werden. Demgegenüber ist die Polizei nicht verpflichtet, sämtliche bei ihr vorhandenen Akten daraufhin zu prüfen, ob in ihnen einzelne Daten vorhanden sind, die nicht mehr benötigt werden. Dies ist faktisch und technisch unmöglich. Hier kann sich die Überprüfungspflicht auf die weitere Notwendigkeit der Akte insgesamt beziehen.[109] Sonstige Daten – insbesondere in Akten – müssen nur vernichtet werden, wenn dadurch nicht andere, noch benötigte Informa-

[97] Die genannten Grundsätze gelten auch für die Fernsehfahndung („Aktenzeichen XY-ungelöst“).

[98] Überblick bei *Frister*, in: Lisken/Denninger (Fn. 7), G Rn. 179 ff.

[99] § 32 NRWPolG. Entsprechend: § 46 BWPolG i.V.m. § 23 BWLDSG; Art. 45 BayPAG; § 48 BerlASOG; § 47 BbgPolG; § 36k HBPolG; § 24 HHPolDVG; § 27 HeSOG; § 45 MVSOG; §§ 39a NdsSOG, 17 NdsLDSG; § 39 RPPOG; § 38 SlPolG; §§ 49 SachsPolG i.V.m. 19-21 SachsLDSG; § 32 LSASOG; § 196 SHLVwG; § 45 ThürPAG; § 35 BPolG; § 24 Nr. 12 NRWOBG; § 23 Nr. 2f BbgOBG.

[100] *Dammann* (Fn. 7), § 3 Rn. 174.

[101] Zu diesen Funktionen der Speicherung siehe oben II. 1.

[102] Näher *Dammann* (Fn. 7), § 3 Rn. 164 ff.

[103] Dazu § 32 Abs. 1 NRWPolG. Entsprechende Landesgesetze s.o. Fn. 42.

[104] Hierzu nochmals oben II. 1.

[105] Nach BVerwG, Buchholz 402.46, Nr. 2, BWVGH NVwZ-RR 2000, 287 (288), kann die Polizei grundsätzlich davon ausgehen, dass die Speicherung personenbezogener Daten bis zum Ablauf der gesetzlich vorgesehenen Regelfristen für eine Überprüfung erforderlich ist. Dies dispensiert m.E. vor allem von der Pflicht, nach nicht mehr benötigten Daten zu suchen; nicht aber davon, nicht mehr benötigte Daten im Falle ihrer Entdeckung im Einzelfall zu löschen.

[106] § 16 Abs. 4 NRWPolG. Entsprechende Landesgesetze s.o. Fn. 12.

[107] Etwa § 17 Abs. 2; § 18 Abs. 2 NRWPolG. Entsprechend: § 22 Abs. 6, § 23 Abs. 3 BWPolG; Art. 33 Abs. 5, Art. 34 Abs. 4 BayPAG; § 25 Abs. 3, 5 BerlASOG; § 33 Abs. 2, § 33a Abs. 4 BbgPolG; § 33 Abs. 3 HBPolG; § 10 Abs. 3 HHPolDVG; § 15 Abs. 3, 5 HeSOG; § 34 Abs. 1-3, § 34b Abs. 5 MVSOG; § 35 Abs. 3-5, § 35a Abs. 4, 5 NdsSOG; § 28 Abs. 5, 6, § 29 Abs. 7 RPPOG; § 28 Abs. 3, 4 SlPolG; § 39 Abs. 3, 4 S. 2 SachsPolG; § 17 Abs. 2 S. 3, Abs. 5 LSASOG; § 186 Abs. 1-3 SHLVwG; § 34 Abs. 6, § 35 Abs. 4, 5 ThürPAG; § 28 Abs. 3 BPolG.

[108] Etwa § 31 Abs. 3 NRWPolG am Beispiel der Rasterfahndung; siehe entsprechend: § 46 Abs. 3 BbgPolG; § 36i Abs. 4 HBPolG; § 23 Abs. 3 HHPolDVG; § 26 Abs. 3 HeSOG; § 44 Abs. 3 MVSOG; § 38 Abs. 4 RPPOG; § 37 Abs. 3 SlPolG; § 47 Abs. 3 S. 3 SachsPolG; § 31 Abs. 3 LSASOG; § 44 Abs. 3 ThürPAG.

[109] Anderes gilt allerdings für Einzelinformationen, welche aus der Akte gewonnen und suchfähig etwa in Karteiform aufbewahrt werden.

tionen in der Akte beeinträchtigt werden. Ihre Vernichtung setzt also die Vernichtbarkeit der ganzen Akte voraus. Dies ist insbesondere nach Ablauf der Aufbewahrungsfristen der Fall.[110] Einzelne Daten aus ihnen sind, wenn sie im Einzelfall entdeckt werden, unter den genannten Voraussetzungen (1)-(3) zu sperren und damit der weiteren polizeilichen Arbeit praktisch zu entziehen. An die Stelle der Löschung kann die Archivierung treten.[111] In diesen Fällen dürfen die Informationen für die Polizeiarbeit nicht mehr genutzt werden. Ihre Benutzung folgt sodann den Regelungen des Archivrechts.

Grenzen der Löschungspflichten entstehen, soweit die Löschung schützwürdige Interessen des Betroffenen beeinträchtigen kann (etwa im Fall von Schadensersatzansprüchen gegen die Behörde oder Dritte), zur Verhinderung einer bestehenden (nicht zukünftigen) Beweisnot oder bei der Notwendigkeit der Datennutzung zu wissenschaftlichen Zwecken. In diesen Fällen sind die Daten zu sperren, also für jeden anderen als den noch zulässigen Zweck nicht mehr nutzbar.

III. Schutzansprüche Betroffener

Personen, deren Daten behördlich verarbeitet werden, können aus Polizei- und Datenschutzgesetzen eine Reihe von subjektiven Rechten herleiten.[112] Deren Durchsetzung, namentlich gegenüber der Polizei, bereitet jedoch erhebliche Schwierigkeiten.

Auskunftsansprüche können Betroffene in die Lage versetzen, überhaupt festzustellen, dass und welche Daten über sie gespeichert sind. Informationsfreiheits- oder Datenschutzgesetze[113] begründen solche Ansprüche, wenn (1) eine öffentliche Stelle, z.B. eine Behörde, (2) personenbezogene Daten über eine Person verarbeitet, sofern (3) durch die Auskunft, weder die Erfüllung der Aufgaben der Behörde noch die öffentliche Sicherheit, noch das Wohl von Bund oder Land beeinträchtigt werden. Letzteres wird bei Polizeibehörden regelmäßig angenommen, ist aber im Einzelfall zu prüfen. Faktisch wird äußerst selten Auskunft erteilt.

Berichtigungsansprüche können Betroffene in die Lage versetzen, falsche Informationen über sie korrigieren zu lassen. Polizei- oder Datenschutzgesetze[114] erkennen solche Ansprüche zu, wenn (1) eine Polizeibehörde (2) personenbezogene Daten über eine Person verarbeitet, (3) welche inhaltlich unrichtig sind. Hierbei geht es um Sachinformationen, nicht hingegen über dadurch ermöglichte oder daraus herzuleitende Wertungen.[115] Bei diesen können allein die tatsächlichen Grundlagen berichtigt werden. Ist die Wertung danach unzulässig, so kann ein Beseitigungsanspruch entstehen.

Löschungsansprüche entstehen aus Polizei- oder Datenschutzgesetzen,[116] wenn (1) eine Polizeibehörde (2) personenbezogene Daten über eine Person verarbeitet, (3) die für ihren Erhebungszweck oder sonstige zulässige Verarbeitungszwecke nicht mehr benötigt wird oder ihre Löschung gesetzlich angeordnet ist.[117]

Die Durchsetzbarkeit dieser Ansprüche bereitet regelmäßig erhebliche Schwierigkeiten, weil Betroffene nicht erfahren, dass über sie Daten erhoben worden sind oder (immer noch) gespeichert sind, oder aber (immer noch) weiter verarbeitet werden. Die Kenntnis davon ist vielfach eher zufällig; gesetzliche Bekanntgabepflichten[118] nach schwerwiegenden Grundrechtseingriffen werden – wenn überhaupt – regelmäßig erst wirksam, wenn die Maßnahme längst abgeschlossen ist und keine weitere zulässige Informationsnutzung mehr in Betracht kommt. Sie ist also kein Instrument wirksamen Rechtsschutzes, sondern ermöglicht allenfalls Fortsetzungsfeststellungsklagen gegen längst abgeschlossene Sachverhalte. Betroffene müssen also die Maßnahmen zunächst hinnehmen und können erst (lange) danach gerichtliche Schritte einleiten. Um solchen Defiziten abzuhelfen, unterliegt die polizeiliche-, wie jede andere behördliche Datenverarbeitung auch, der objektiv-rechtlichen Kontrolle durch Bundes- und Landesdatenschutzbeauftragte.[119]

---

[110] § 32 Abs. 3 NRWPolG. Entsprechend: § 46 Abs. 1 BWPolG; Art. 45 Abs. 2 BayPAG; § 48 Abs. 2, 3 Berl-ASOG; § 47 Abs. 2, 3 BbgPolG; § 36k Abs. 2, 3 HBPolG; § 24 Abs. 2 S. 3, Abs. 3 HHPolDVG; § 27 Abs. 2, 3 HeSOG; § 45 Abs. 2, 3 MVSOG; § 39a NdsSOG, § 17 Abs. 2 NdsLdSG; § 39 Abs. 2 RPPOG; § 38 Abs. 2 SlPolG; §§ 49 SachsPolG i.V.m. 20 Abs. 2 SachsLDSG; § 32 Abs. 2, 3 LSASOG; § 45 Abs. 2 ThürPAG; § 35 Abs. 2, 5 BPolG.

[111] § 32 Abs. 6 NRWPolG, zum Archivrecht *Ladeur*, in: Hoffmann-Riem u.a. (Fn. 2), § 21 Rn. 36 ff.

[112] Zur Belehrungs- oder Informationspflichten näher *Petri* (Fn. 7), H Rn. 544 ff.

[113] Z.B. § 18 NRWDSG. Entsprechend: § 21 BWDSG; § 16 BerlDSG; § 18 HeDSG; § 13 ThürDSG; § 20 SlDSG; § 27 SHLDSG; § 24 MVDSG; Art. 10 BayDSG; § 18 BbgDSG; § 16 BerlDSG; § 16 NdsDSG; § 18 HHDSG; § 18 SachsDSG; § 15 LSADSG; § 21 HBDSG; § 18 RPDSG; § 19 BDSG; siehe dazu *Petri* (Fn. 7), H Rn. 551 ff.; *Weichert*, NVwZ 2007, 1004; Einzelfall: BGH JZ 2007, 48 (50) m. Anm. *Perron*.

[114] § 32 Abs. 1 NRWPolG. Entsprechende Landesgesetze s.o. Fn. 42.

[115] Dazu § 23 Abs. 2 NRWPolG. Entsprechend: § 43 Abs. 2 BerlASOG; § 38 Abs. 2 BbgPolG; § 36a Abs. 3 HBPolG; § 14 Abs. 3 HHPolDVG; § 36 Abs. 2 MVSOG; § 30 Abs. 4 SlPolG; § 188 Abs. 2 SHLVwG; § 29 Abs. 4 BPolG.

[116] Siehe § 32 NRWPolG. Entsprechende Landesgesetze siehe Fn. 99.

[117] Dazu näher oben II. 4.

[118] Etwa: § 20w BKAG; § 17 Abs. 5 NRWPolG, siehe entsprechend: § 22 Abs. 8 BWPolG; Art. 33 Abs. 7 S. 1, 2 BayPAG; § 25 Abs. 7, 7a BerlASOG; § 29 Abs. 8 BbgPolG; § 33 Abs. 5 S. 1 HBPolG; § 10 Abs. 6 S. 1 HHPolDVG; § 34 Abs. 5, 6 MVSOG; § 30 Abs. 4, 5 NdsSOG; § 40 Abs. 5, 6 RPPOG; § 28 Abs. 5 SlPolG; § 39 Abs. 8, 9 SachsPolG; § 17 Abs. 7, 8 LSASOG; § 186 Abs. 4 S. 1-4, Abs. 5 SHLVwG; § 34 Abs. 9, 10 ThürPAG; § 28 Abs. 5 BPolG. Dazu *Petri* (Fn. 7), H Rn. 549 f.

[119] Dazu § 1 Abs. 1, 2, 4 f., § 38 BDSG, entsprechend: §§ 1, 28 BWDSG; §§ 1, 24 HeDSG; §§ 1, 26 SLDSG; §§ 1, 39 SHLDSG; §§ 1, 30 MVDSG; Art. 1, 30 BayDSG; §§ 1, 23 BbgDSG; §§ 1, 24 BerlDSG; §§ 1, 22 NdsDSG; §§ 1, 22 NRWDSG; §§ 1, 23 HHDSG; §§ 1, 37 ThürDSG; §§ 1, 27

Äußerst schwierige und umstrittene Fragen stellen sich gegenwärtig hinsichtlich der Frage möglicher Verarbeitungs- und Verwertungsverbote bei rechtswidriger Informationserhebung. Grundannahme der in jüngerer Zeit nur noch selten systematisch erforschten Thematik ist die Aussage, wonach rechtswidrig erhobene Informationen rechtlich nicht einfach genauso behandelt werden dürfen wie rechtmäßig erhobene. Schwieriger ist es allerdings, die dadurch notwendig werdenden Differenzierungen sowie die zu ihrer Begründung notwendigen rechtlichen Kriterien zu ermitteln. Gefordert werden grundgesetzkonforme gesetzliche Regelungen. Für das Strafprozessrecht geht das Bundesverfassungsgericht in einer Serie von Beschlüssen davon aus, dass die Bewältigung der Folgen rechtswidriger Beweiserhebung grundsätzlich eine Aufgabe des Gesetzgebers und der Fachgerichte sei.[120] Insbesondere wird die Geltung eines grundgesetzlichen Rechtssatzes verneint, wonach im Falle einer rechtswidrigen Beweiserhebung die Verwertung der gewonnen Beweise *stets* unzulässig sei. Ein solcher Rechtssatz könne daher dem Strafprozessrecht vom Grundgesetz auch nicht vorgegeben sein. Die Auffassung der Strafgerichte, wonach im Einzelfall eine Abwägung zwischen dem Strafverfolgungsinteresse und -anspruch einerseits sowie den betroffenen Grundrechten andererseits geboten und zulässig sei, wird nicht beanstandet. Ein Beweisverwertungsverbot sei jedenfalls erst geboten, wenn „die zur Fehlerhaftigkeit der Ermittlungsmaßnahme führenden Verfahrensverstöße schwerwiegend waren oder bewusst oder willkürlich begangen wurden."[121] So zutreffend der genannte Ausgangspunkt sein mag, wonach nicht jede (!) Verletzung von Form- oder Verfahrensvorschriften bei der Informationserhebung ein Verwertungsverbot begründet, so überprüfungsbedürftig ist doch die daraus hergeleitete Konsequenz, dass die Rechtsverletzung stets eine schwerwiegende sein müsse. Was zunächst wie ein Bagatellvorbehalt anmutete, wird so ohne Begründung zu einem Qualifikationstatbestand von Eingriffsmaßnahmen, dem nicht nur die verfassungsrechtliche Begründung, sondern insbesondere auch die Leistungsfähigkeit als Abgrenzungskriterium weitgehend abgeht. So hat die bisherige Rechtsprechung weder befriedend gewirkt noch konsentierte Maßstäbe herausgearbeitet.

Für das Recht der Gefahrenabwehr kann festgehalten werden: Die Befugnisnormen zur Informationsverarbeitung beziehen sich auf rechtmäßig erhobene Daten.[122] Demnach dürfen auch nur sie verarbeitet werden. Dementsprechend entstehen für rechtswidrig verarbeitete Informationen ein Verarbeitungsverbot und ein Verwertungsverbot.[123] Ausnahmen davon können gesetzlich angeordnet werden, wenn (1) eine Information mit freiwilliger (!) Zustimmung des Betroffenen verwendet wird (etwa zu seiner Entlastung), oder (2) eine Information zum Schutz überragend wichtiger Rechtsgüter verwendet wird und ihre Verwendung auf diesen Zweck beschränkt wird. Dies gilt allerdings nur für schon vorhandene und noch nicht gelöschte Informationen, die Löschungspflicht bleibt daneben bestehen. Eine (rechtswidrige) Erhebung zu diesem Zweck bleibt unzulässig. In neuen Gesetzen wird dieser Ausnahmetatbestand teilweise schon bei der Informationserhebungsbefugnis berücksichtigt.[124]

IV. Zusammenfassung

Polizeiliche Tätigkeit ist zentral Informationsverarbeitung. Diese ist nach allgemeinen Grundsätzen des Verwaltungsorganisations- und -informationsrechts zulässig. Besondere Anforderungen entstehen bei der Verarbeitung personenbezogener Daten.

Polizei- und Datenverarbeitungsrecht unterscheiden als Verarbeitungsformen die Datenerhebung, -speicherung, -veränderung, -übermittlung und -löschung. Einerseits kennen die Gesetze eine Rechtspflicht zur Datenverarbeitung. Andererseits hat diese in dem Rahmen der durch Grundrechte und Gesetze gezogenen Grenzen zu erfolgen. Dies erfordert im Einzelfall schwierige Abwägungen, welche durch besondere Überprüfungs- und Fristenregelungen formalisiert werden. Den daraus entstehenden behördlichen Pflichten korrespondieren Ansprüche Betroffener, die von ihnen allerdings mangels Kenntnis der einzelnen Verarbeitungsvorgänge und -dauern kaum je durchzusetzen sind.

Grundsätzlich dürfen nur rechtmäßig erlangte Informationen verarbeitet werden. Hinsichtlich rechtswidrig erlangter Daten ist das früher regelmäßig angenommene Verwertungsverbot inzwischen wohl nur noch der Regelfall, welcher jedenfalls bei entsprechender gesetzlicher Regelung durch einzelne Ausnahmen durchbrochen werden darf. Die dafür maßgeblichen grundgesetzlichen Vorgaben sind gegenwärtig aber noch schwer erkennbar.

SachsDSG; §§ 1, 22 LSADSG; §§ 1, 27 HBDSG; §§ 1, 24 RPDSG.

[120] BVerfG NJW 2008, 3053 (3054); jüngst BVerfG, Beschl. v. 2.7.2009 – 2 BvR 2225/08 = HRRS 2009 Nr. 648. Zu Folgefragen etwa *Daleman/Heuchemer,* JA 2003, 430.

[121] BVerfGE 113, 29 (61); NJW 1999, 273 (274); NJW 2006, 2684 (2686); NJW 2009, 3225 (3226).

[122] Dazu o. I. 1., II. vor 1.

[123] Grundlegend und zutreffend *Störmer*, Dogmatische Grundlagen der Verwertungsverbote, 1992; wesentlich weiter differenzierend als hier *Würtenberger/Heckmann* (Fn. 1), Rn. 655 ff.

[124] So ansatzweise etwa § 20c Abs. 3; § 20u Abs. 2 BKAG.