# Datenschutzaufsicht im strafprozessualen Ermittlungsverfahren

*von Mathias Gisch**

*Abstract*
*Mit einer gewissen Regelmäßigkeit finden sich in den Tätigkeitsberichten der Landesbeauftragten für Datenschutz Schilderungen über mangelnde Unterstützung von Seiten der Staatsanwaltschaften und der Polizei im Rahmen der Wahrnehmung von aufsichtsrechtlichen Befugnissen bei datenschutzrechtlichen Prüfungen in laufenden strafprozessualen Ermittlungsverfahren. Teilweise wird eine datenschutzrechtliche Prüfungsbefugnis im laufenden Ermittlungsverfahren ganz abgelehnt[1], teilweise besteht Uneinigkeit über Art und Umfang der Kontrollbefugnisse der Landesdatenschutzbeauftragten.[2] In einer anderen Konstellation verweigert die Polizei unter Verweis auf die Staatsanwaltschaft und deren strafprozessualen Verfahrensherrschaft eine Zusammenarbeit mit der Landesbeauftragten für Datenschutz.[3] Im Folgenden sollen die rechtlichen Grundlagen für die Zuständigkeit der Landesbeauftragten für Datenschutz dargestellt werden und sodann auf die datenschutzrechtlich zulässigen Untersuchungs- und Abhilfebefugnisse eingegangen werden, bevor hieraus Schlussfolgerungen für die Ausübung der Aufsicht gegenüber der (repressiv tätigen) Polizei und Staatsanwaltschaft gezogen werden.*

*With a certain regularity, the activity reports of the state commissioners for data protection contain descriptions of insufficient support from the public prosecutor's offices and the police in the context of exercising supervisory powers in data protection audits in ongoing criminal investigations. In some cases, the authority of the state commissioners to review processing activities under data protection law is completely refused in the course of the ongoing investigation; in some cases, there is disagreement about the type and scope of the control powers of the state commissioners. In another constellation, the police refused to cooperate with the state commissioner for data protection, referring to the public prosecutor's office and their procedural rule. In the following, the legal basis for the competence of the state commissioners for data protection is presented and then their investigative and corrective powers permitted under data protection law are discussed before conclusions for the exercise of supervision vis-à-vis the (repressive) police and public prosecutor's office are drawn from this.*

## I. Zuständigkeit der Landesbeauftragten für Datenschutz

Die Zuständigkeit der Landesbeauftragten für Datenschutz im strafprozessualen Ermittlungsverfahren ergibt sich aus einem Zusammenspiel aus verfassungsrechtlichen und europarechtlichen Vorgaben, die in der StPO umgesetzt und im jeweiligen Landesrecht konkretisiert werden.

### *1. Verfassungsrechtliche Vorgaben*

Verfassungsrechtliche Vorgaben für die Existenz und Ausgestaltung der datenschutzrechtlichen Aufsicht ergeben sich aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) und dessen objektivrechtlicher Dimension. Diese objektivrechtliche Dimension der Grundrechte allgemein beinhaltet unter anderem die Pflicht des Gesetzgebers in Form von privatrechtlichen Einrichtungen (Institutsgarantien[4]) oder öffentlich-rechtlichen Einrichtungen (institutionelle Garantien[5]) ein Norm- und Regelungsgefüge („grundrechtsfreundliches ‚Regelungsambiente'"[6]) zu schaffen, das Bedrohungen des betroffenen Grundrechts begegnet und einem Substanzverlust entgegenwirkt.[7]

Bezogen auf das Recht auf informationelle Selbstbestimmung und vor dem Hintergrund, dass die Verarbeitung, insbesondere die Verwendung, einmal erhobener personenbezogener Daten weitgehend losgelöst von der betroffenen Person stattfindet, konkretisiert das *BVerfG* im sog. Volkszählungsurteil diese objektivrechtliche Dimension betreffend die Datenverarbeitung öffentlicher Stellen dahingehend, dass es eine organisatorische Absicherung des Grundrechtsschutzes in Form der Institutionalisierung entsprechender Kontrollinstanzen fordert:

"Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung."[8]

---

* *Mathias Gisch* ist Leiter des Referats Polizeiliche Datenverarbeitung bei der Landesbeauftragten für Datenschutz und Informationsfreiheit Saarland.

1 Der Bayerische Landesbeauftragte für den Datenschutz Bayern, 18. Tätigkeitsbericht 1997/98, Ziff. 5.10.

2 Bericht des Unabhängigen Landeszentrums für den Datenschutz Schleswig-Holstein, 23. Tätigkeitsbericht 2001, Ziff. 4.3.5.

3 Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Pressemitteilug vom 20.8.2019: „Automatische Kennzeichenfahndung: Datenschutzbeauftragte beanstandet mangelnde Unterstützung durch das Polizeipräsidium Brandenburg".

4 *Herdegen,* in: Maunz/Dürig, GG, 91. Aufl. (2020), Art. 1 Abs. 3 Rn. 19.

5 A.a.O.

6 *Herdegen,* in: Maunz/Dürig, GG, Art. 1 Abs. 3 Rn. 24.

7 *Herdegen,* in: Maunz/Dürig, GG, Art. 1 Abs. 3 Rn. 23.

8 *BVerfG*, Urt. v. 15.12.1983, BVerfGE 65, 1 (46).

Die Betonung des Adjektivs „*vorgezogen*“ macht dabei deutlich, dass das *BVerfG* die Kontrollaufgaben dieser Institution als solche mit präventiver Schwerpunktsetzung ansieht. Dass die Maßnahme einer Strafverfolgungsbehörde nachträglich gerichtlich überprüft werden kann (wie im Übrigen jede Maßnahme einer staatlichen Stelle), ist dementsprechend nicht schon ausreichend. Die Datenschutzbeauftragten sollen, wie es in einem vier Jahre nach dem Volkszählungsurteil erlassenen Beschluss[9] zum dann neu gefassten Volkszählungsgesetz[10] präzisiert wird, bereits frühzeitig durch die datenverarbeitenden Stellen beteiligt werden, um mit jenen gemeinsam die zur „grundrechtsschützenden und -wahrenden Durchführung erforderlichen technischen und organisatorischen Maßnahmen [...] rechtzeitig zu entwickeln“[11] und diese zu kontrollieren. Die Funktion der Datenschutzkontrolle besteht damit darin, den sich aus der Datenverarbeitung ergebenden Gefahren bereits im Vorfeld der Verarbeitung zu begegnen und die Einhaltung der gesetzlichen Vorgaben durch die datenverarbeitende Stelle zu überwachen und sicherzustellen, unabhängig vom Vorliegen einer konkreten Betroffenheit.

Die Akzentuierung einer vorbeugenden institutionalisierten Kontrolle bedeutet allerdings nicht, dass sich die Funktion der Datenschutzbeauftragten in einer Beteiligung im Vorfeld der Realisierung eines Verarbeitungsverfahrens erschöpft. Effektiver Schutz des Rechts auf informationelle Selbstbestimmung bedeutet auch, dass die Datenschutzbeauftragten sowohl anlasslos als auch – selbstverständlich – anlassbezogen konkrete Verarbeitungsabläufe auf ihre Rechtmäßigkeit hin überprüfen und bei festgestellten Verstößen gegenüber den verantwortlichen Stellen – in unterschiedlicher Weise – auf eine Abhilfe hinwirken können.[12] Hierzu bedarf es der Normierung von exekutiven Befugnissen und Durchsetzungskompetenzen. Wie diese Einwirkungsbefugnisse im Einzelnen auszugestalten sind, dazu macht das *BVerfG* keine Vorgaben, so dass dies dem Gestaltungsspielraum des Gesetzgebers überlassen ist. Dem Gesetzgeber bleibt es dabei unbenommen, die Zuweisung entsprechender Befugnisse adressatengerecht auszugestalten, solange dabei die Wirksamkeit der Kontrolle gewahrt bleibt.[13] Deutlich wird dies am Beispiel der sektoralen Differenzierung von Datenverarbeitungen durch öffentliche und nichtöffentliche Stellen. Während es im nichtöffentlichen Bereich zur Durchsetzung eines wirksamen Datenschutzes exekutiver Anordnungsbefugnisse in Form von bspw. Löschungs- oder Unterlassungsanordnungen bedarf, beschränkten sich die Einwirkungskompetenzen im öffentlichen Bereich bisher auf die Festlegung von Beanstandungs-, Beratungs- und Berichtskompetenzen. Dahinter steht der Gedanke, dass die Pflicht zur Beachtung datenschutzrechtlicher Bestimmungen für die öffentlichen Stellen bereits unmittelbar aus dem Grundsatz der Gesetzmäßigkeit der Verwaltung folgt und dass es insofern lediglich einer „Erinnerung“ bedarf, um die datenverarbeitende Stelle, möglicherweise unter Beteiligung der jeweiligen Rechtsaufsichtsbehörde, zu einer Abstellung rechtswidriger Datenverarbeitungsvorgänge zu bewegen.

Die in der Vergangenheit im öffentlichen Bereich vorgesehene Beschränkung auf Beanstandungskompetenzen ist indes nicht zwingend. Ganz im Gegenteil ist der neueren Rechtsprechung des *BVerfG* zu entnehmen, dass die Kompetenz zur Beanstandung eher zu den verfassungsrechtlich erforderlichen Essentialia gehört.[14] Die darüber hinausgehende Festlegung weitergehender exekutiver Anordnungsbefugnisse auch gegenüber öffentlichen Stellen schließt das *BVerfG* nicht aus, sondern überlässt dies dem Beurteilungsspielraum des Gesetzgebers. Im Rahmen dieses Beurteilungsspielraums kann sich die Notwendigkeit zur Normierung weitergehender Kompetenzen insbesondere aus europarechtlichen Vorgaben ergeben.

### *2. Europarechtliche Vorgaben*

Die europarechtlichen Rahmenbedingungen für die Ausgestaltung der datenschutzrechtlichen Aufsicht auch in strafprozessualen Ermittlungsverfahren ergeben sich aus der Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie, JI-RL). Nach Art. 2 JI-RL gilt die Richtlinie für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden sollen, zum Zwecke der Strafverfolgung, Strafvollstreckung und dem Schutz vor und Abwehr von Gefahren für die öffentliche Sicherheit durch die zuständigen Behörden.

#### *a) Automatisierte/nichtautomatisierte Verarbeitung*

Bezogen auf das strafrechtliche Ermittlungsverfahren finden die Vorschriften der JI-Richtlinie somit zunächst unzweifelhaft dann Anwendung[15], wenn im Rahmen eines Ermittlungsverfahrens personenbezogene Daten in Vorgangs- oder Fallbearbeitungssystemen (bspw. POLADIS, Web.StA) verarbeitet werden. Darüber hinaus gilt die JI-Richtlinie aber auch dann, wenn ganz oder teilweise automatisierte Ermittlungstechniken, wie beispielsweise Telekommunikationsüberwachung (§ 100a StPO), Online-Durchsuchung (§ 100b StPO), KFZ-Kennzeichenerfassung (§ 100h StPO), IMSI-Catcher (§ 100i StPO) oder auch elektronische Auswerteverfahren bis hin zu BigData-Analysen zur Strafverfolgung zum Einsatz kommen.

---

9 *BVerfG*, Beschl. v. 24.9.1987 – 1 BvR 970/87 = NJW 1987, 2805.

10 Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1987) vom 8.11.1985 (BGBl. I, S. 2078 ff.).

11 *BVerfG*, Beschl. v. 24.9.1987 – 1 BvR 970/87 = NJW 1987, 2805 (2806).

12 *Albers*, Informationelle Selbstbestimmung, 2005, S. 476.

13 A.a.O.

14 *BVerfG*, Urt. v. 19.5.2020 – 1 BvR 2835/17, Rn. 276.

15 Wegen der Richtlinienform bedarf es grds. der vorherigen Umsetzung der europarechtlichen Vorgaben in nationales Recht.

Schließlich fällt auch die manuelle Verarbeitung von personenbezogenen Daten, die im Rahmen einer noch nicht elektronisch bzw. noch gegenständlich geführten Ermittlungsakte erfolgt, in den Anwendungsbereich der JI-Richtlinie, da es sich bei der klassischen Ermittlungsaktenführung um ein Dateisystem i.S.d. Art. 3 Nr. 6 JI-RL handelt. Ein Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten geordnet oder geführt wird. Unter einer Sammlung wiederum ist die planmäßige Zusammenstellung einzelner Angaben zu verstehen, die einen inneren Zusammenhang vorweist, der sich entweder aus der Gleichartigkeit der Informationen oder – wie hier – der Gleichartigkeit des Zwecks (jeweils konkretes Ermittlungsverfahren) ergibt.[16] Ein strukturierter, d.h. gleichartiger Aufbau liegt bereits dann vor, wenn Akten nach ihrer äußeren Beschriftung ein gleiches System beinhalten. Auf einen gleichartigen inneren Aufbau der Akte kommt es dann nicht mehr an.[17] Zugänglich ist eine solche Sammlung dann, wenn durch diesen formalen Aufbau die Daten leichter erschlossen werden können, sprich ordnungsfähig sind; nicht entscheidend ist, ob die Sammlung auch tatsächlich geordnet ist. Ebenso wenig muss eine Auswertbarkeit gegeben sein.[18]

Bei der noch gegenständlich geführten Ermittlungsakte sind diese Kriterien gewiss erfüllt. Das der Ermittlungsakte zugrungeliegende Ordnungsschema besteht zumindest aus Angaben zur Person des Beschuldigten (Name, Geburtsdatum, Nationalität), ggfls. zur Person des Anzeigenerstatters/Strafantragsstellers, dem Tatvorwurf in Form des vorgeworfenen Straftatbestandes sowie Angaben zur innerbehördlichen Organisation (Aktenzeichen, Dezernent, Sachgebiet) und ist damit gleichartig aufgebaut und nach diesen Kriterien zugänglich.

*b) Zuständige Behörde*

Weiterhin findet die JI-Richtlinie nur auf die Datenverarbeitung durch die „*zuständigen Behörden*" Anwendung. Das Merkmal der „*zuständigen Behörde*" (Art. 3 Nr. 7 JI-RL) soll den Anwendungsbereich der JI-Richtlinie begrenzen, indem nur die Datenverarbeitung solcher, vor allem *staatlicher* Stellen erfasst ist, die vom Mitgliedsstaat ausdrücklich mit der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit betraut worden sind (Art. 2 Nr. 7 lit. a JI-RL). Für alle anderen (öffentlichen oder privaten) Stellen, die personenbezogene Daten zum vorgenannten Zweck verarbeiten, denen aber entsprechende hoheitliche Befugnisse nicht vom Mitgliedsstaat übertragen wurden (Art. 2 Nr. 7 lit. b JI-RL), beurteilt sich die datenschutzrechtliche Zulässigkeit ausschließlich anhand der DSGVO.[19]

Nach § 152 Abs. 2 StPO haben die Staatsanwaltschaften die Pflicht, Straftaten zu verfolgen. Nach § 163 Abs. 1 StPO gilt eine hiermit korrespondierende Ermittlungspflicht für die Behörden und Beamten des Polizeidienstes. Beide, sowohl Staatsanwaltschaft als auch Polizei, unterfallen daher, soweit sie repressiv handeln, dem Anwendungsbereich der JI-Richtlinie.

*c) Institutionalisierung der Datenschutzaufsicht*

Konsequenz aus der Anwendbarkeit der JI-Richtlinie ist, dass die Überwachung der Anwendung der JI-Richtlinie bei der Datenverarbeitung durch die zuständigen Behörden bzw. konkret bei den datenschutzrechtlich Verantwortlichen (Art. 2 Nr. 8 JI-RL) durch unabhängige Aufsichtsbehörden gewährleistet werden muss (Art. 41 Abs. 1 JI-RL). Ihnen stehen dabei gegenüber den Verantwortlichen die in Art. 47 JI-RL genannten Untersuchungs- und Abhilfebefugnisse zu (Art. 45 JI-RL).

Die Datenverarbeitung durch die Polizei und Staatsanwaltschaft im Rahmen strafprozessualer Ermittlungsverfahren unterfällt folglich der Zuständigkeit der in Art. 41 JI-RL genannten Aufsichtsbehörde. Für die Staatsanwaltschaft ergibt sich auch nichts Gegenteiliges aus Art. 45 Abs. 2 JI-RL, da Staatsanwaltschaften keine Gerichte sind und auch nicht eine gerichtsähnliche oder richterliche Unabhängigkeit genießen.

Wenngleich die Vorschriften der JI-Richtlinie auch auf die Tätigkeit der Gerichte grundsätzlich Anwendung finden[20], so gilt dies ausnahmsweise nicht für die Regelungen über die Zuständigkeit der Aufsichtsbehörde. Nach Art. 45 Abs. 2 Satz 1 JI-RL sehen die Mitgliedstaaten vor, dass die nach Art. 44 JI-RL zu errichtende Aufsichtsbehörde nicht für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen zuständig ist. Darüber hinaus *kann* der Mitgliedstaat auch solche Verarbeitungen von der Überwachung durch die Aufsichtsbehörde ausnehmen, die andere, unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit vornehmen (Art. 45 Abs. 2 S. 2 JI-RL). Erwägungsgrund 80 erwähnt die Staatsanwaltschaft beispielhaft.

Für die deutsche Staatsanwaltschaft jedenfalls findet diese Vorschrift indes keine Anwendung. Unabhängig von der Frage, ob man das Handeln der Staatsanwaltschaft überhaupt als „*justizielle Tätigkeit*" einordnen kann, oder ob nicht vielmehr das Handeln der Staatsanwaltschaft als ein der Rechtspflege zugeordneter Teil der Exekutive zu verstehen ist, fehlt es bereits an der von Art. 45 Abs. 2 S. 2 JI-RL vorausgesetzten Unabhängigkeit. Hierzu hat der *EuGH* unlängst ausgeführt, dass die deutschen Staatsanwaltschaften keine hinreichende Gewähr für eine Unabhängigkeit gegenüber der Exekutive bieten, da die struk-

---

16 Zur gleichlautenden Definition des Dateisystems in der DSGVO: *Raab,* in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. (2020), Art. 4 Nr. 6 Rn. 3.

17 *Schild*, in: BeckOK-DatenschutzR/DS-GVO, 33. Ed. (1.8.2020), Art. 4 Rn. 83.

18 *Raab,* in: Kühling/Buchner, DS-GVO/BDSG, Art. 4 Nr. 6 Rn. 5.

19 *Sydow*, Europäische Datenschutzgrundverordnung, 2. Aufl. (2018), Art. 2 Rn. 15.

20 ErwGr. 80 JI-RL.

turelle Gefahr bestehe, dass ihr Handeln durch unmittelbare oder mittelbare Weisungen oder Anordnungen des Justizministers beeinflusst werden könnte.[21]

*3. Bundesrechtliche Umsetzung*

Die vorgenannten verfassungs- und europarechtlichen Vorgaben hat der Bundesgesetzgeber in § 500 StPO im Rahmen des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20.11.2019[22] aufgegriffen und die Aufsicht durch die Landesbeauftragten für Datenschutz ausdrücklich angeordnet, soweit öffentliche Stellen der Länder personenbezogene Daten im Anwendungsbereich der StPO verarbeiten. Dabei hat der Bundesgesetzgeber es insbesondere auch unterlassen von der fakultativen Öffnungsklausel des Art. 45 Abs. 2 Satz 2 JI-RL Gebrauch zu machen.

Was die materiellen Regelungen zur Datenverarbeitung im Bereich der Strafverfolgung angeht, ordnet § 500 Abs. 1 StPO eine entsprechende Geltung des dritten Teils des Bundesdatenschutzgesetzes an; die dortigen Vorschriften werden als Auffangvorschrift jedoch durch etwaige bereichsspezifische, abweichende oder ergänzende Regelungen der StPO verdrängt.[23]

Was die datenschutzrechtliche Aufsicht anbelangt, regelt die StPO in § 500 zwar, dass eine Aufsicht durch die Landesbeauftragten für Datenschutz zu erfolgen hat, überlässt die inhaltliche Ausgestaltung dieser Aufsicht aber den jeweiligen Landesgesetzgebers, um so eine „landesspezifische einheitliche Aufsicht der Staatsanwaltschaften und der übrigen öffentlichen Stellen (Anm.: des jeweiligen Bundeslandes) sicherzustellen."[24]

*4. Zwischenergebnis*

Auch im strafprozessualen Ermittlungsverfahren ist eine datenschutzrechtliche Aufsicht durch die Landesbeauftragte für Datenschutz sicherzustellen. Dies gilt unzweifelhaft bei der Polizei. Nach den obigen Ausführungen hat der Gesetzgeber eine solche Aufsicht aber auch bei der Staatsanwaltschaft vorgesehen.

**II. Art und Umfang der Aufsicht**

Nachdem die grundsätzliche Zuständigkeit der Landesbeauftragten für Datenschutz für Datenverarbeitungen, die im Ermittlungsverfahren stattfinden, feststeht, ist noch zu klären, in welcher Art und in welchem Umfang und gegenüber welcher konkreten Stelle die datenschutzrechtliche Aufsicht erfolgt.

*1. Europarechtliche Rahmenbedingungen*

Art. 45 Abs. 1 JI-RL sieht vor, dass sichergestellt sein muss, dass die Aufsichtsbehörde, die ihr gemäß der JI-Richtlinie zugewiesenen Aufgaben und übertragenen Befugnisse zu erfüllen hat. Es ist dabei durch den mitgliedstaatlichen Gesetzgeber zu gewährleisten, dass die Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig handelt (Art. 42 Abs. 1 JI-RL).

*a) Aufgaben*

Die Aufgaben der Aufsichtsbehörde sind in Art. 46 JI-RL aufgezählt. Auch im Ermittlungsverfahren hat die Aufsichtsbehörde die Anwendung der nach der JI-Richtlinie erlassenen Vorschriften zu überwachen und durchzusetzen (Art. 46 Abs. 1 lit. a JI-RL), die Verantwortlichen für die ihnen aus der JI-Richtlinie entstehenden Pflichten zu sensibilisieren (Art. 46 Abs. 1 lit. d JI-RL), sich mit Beschwerden einer betroffenen Person zu befassen und den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen (Art. 46 Abs. 1 lit. f JI-RL), die Rechtmäßigkeit der Verarbeitung gemäß Art. 17 JI-RL zu überprüfen und Untersuchungen über die Anwendung der JI-RL durchzuführen (Art. 46 Abs. 1 lit. i JI-RL), um nur Einige zu nennen.

*b) Befugnisse*

Zur Wahrnehmung dieser Aufgaben hat der Mitgliedstaat die nach Art. 47 JI-RL vorgesehenen Befugnisse zugunsten der Aufsichtsbehörde in Rechtsvorschriften zu normieren. Die JI-Richtlinie unterscheidet hierbei zwischen Untersuchungs-, Abhilfe-, Genehmigungs-/Beratungs- sowie Klage-/Beschwerdebefugnissen.

Die in Art. 47 Abs. 1 JI-RL vorgesehen Untersuchungsbefugnisse sollen es der Aufsichtsbehörde ermöglichen zunächst den datenschutzrechtlich relevanten Sachverhalt zu ermitteln. Hierzu hat die Aufsichtsbehörde die Befugnis von dem Verantwortlichen und/oder dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und auf alle Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten.

Die in Art. 47 Abs. 2 JI-RL als Mindeststandard vorgesehenen Abhilfebefugnisse zielen demgegenüber darauf ab, bei einem festgestellten datenschutzrechtlichen Verstoß beim Verantwortlichen für die Zukunft auf ein datenschutzkonformes Vorgehen hinzuwirken.

Die Beratungsbefugnisse ergeben sich aus Art. 47 Abs. 3 JI-RL. Neben der Beratung im Zusammenhang mit der Durchführung einer Datenschutzfolgenabschätzung und einer daraus resultierenden Notwendigkeit der vorherigen Konsultation nach Art. 28 JI-RL, eröffnet Art. 47 Abs. 3 JI-RL der Aufsichtsbehörde insbesondere auch die Möglichkeit sich zu datenschutzrechtlichen Fragen im Zusammenhang mit der Verarbeitung personenbezogener Daten für Zwecke der JI-Richtlinie an den Landtag und/oder die Regierung zu wenden. In eine ähnliche Richtung deutet Art. 47 Abs. 5 JI-RL, der es der Aufsichtsbehörde ermöglicht, datenschutzrechtliche Verstöße den Justizbehörden

21 *EuGH*, Urt. v. 27.5.2019 – C 508/18.
22 BGBl. I, S. 1724.
23 BT-Drs. 19/4671, S. 71.
24 BT-Drs. 19/4671, S. 71.

zur Kenntnis zu bringen. In den beiden letztgenannten Fällen handelt es sich streng genommen ebenfalls um Abhilfebefugnisse, die aber, anders als jene nach Art. 47 Abs. 2 JI-RL, nicht unmittelbar gegenüber dem Verantwortlichen ausgeübt werden, sondern (nur) mittelbar eine datenschutzkonforme Anpassung der Verarbeitung personenbezogener Daten erreichen wollen.

*c) Unabhängigkeit*

Bei der Wahrnehmung der Aufgaben und Befugnisse der Aufsichtsbehörde ist zudem sicherzustellen, dass die Aufsichtsbehörde völlig unabhängig handelt. Bereits im Jahr 2010 hat der *EuGH* zum Erfordernis der „völligen Unabhängigkeit" festgestellt, dass hierbei gewährleistet sein muss, dass die Aufsichtsbehörde „ihre Aufgaben ohne äußere Einflussnahme [wahrnehmen kann]. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen."[25]

*2. Bundes- und landesrechtliche Konkretisierung*

Wie bereits oben ausgeführt trifft § 500 StPO i.V.m. dem dritten Teil des BDSG nur materiell-rechtliche Vorgaben für die Verarbeitung personenbezogener Daten im Ermittlungsverfahren. Konkrete Regelungen zu Art und Umfang der Befugnisse der Aufsichtsbehörde sind der StPO und dem dritten Teil des BDSG nicht zu entnehmen.[26] Zwar sieht § 68 BDSG i.V.m. § 500 Abs. 1 Nr. 2 StPO eine Pflicht zur Zusammenarbeit des Verantwortlichen mit der Aufsichtsbehörde vor. Die Vorschrift setzt Art. 26 JI-RL um. Nach allgemeiner Auffassung hat sie jedoch kaum praktische Bedeutung, da der Gesetzgeber nach Art. 47 JI-RL verpflichtet ist, der Aufsichtsbehörde wirksame Befugnisse einzuräumen, die gegenüber der allgemeinen Regelung des § 68 BDSG spezieller und vorrangig sind.[27] Die konkrete Umsetzung der aufsichtlichen Befugnisse überlässt der Bundesgesetzgeber mit dem Argument eine landeseinheitliche Aufsicht ermöglichen zu wollen, ausdrücklich dem Landesgesetzgeber.[28]

*a) Festlegung der Aufsichts- und Kontrollbefugnisse im Landesrecht*

Der Umfang der zulässigen aufsichtsbehördlichen Befugnisse – das „Wie" der Aufsicht – ergeben sich für die Landesbeauftragten für Datenschutz aus dem jeweiligen Landesrecht, das – der Rechtsform der Richtlinie geschuldet – einer am Maßstab der Art. 47 JI-RL erfolgenden Ausgestaltung durch den Gesetzgeber bedarf.

Mit den aufsichtsbehördlichen Befugnissen korrespondiert im Regelfall eine Mitwirkungspflicht auf Seite der verantwortlichen und beaufsichtigten Stelle. Danach sind die öffentlichen Stellen der Länder in unterschiedlicher Weise verpflichtet, die Landesbeauftragten für Datenschutz und deren Beauftragte bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere Auskunft auf die Fragen zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, sowie jederzeit – auch unangemeldet – ungehinderten Zutritt zu allen Diensträumen zu gewähren.

*b) Vorrang der §§ 474 ff. StPO?*

Hierbei stellt sich jedoch die Frage, ob die durch Landesgesetz normierten aufsichtsbehördlichen Befugnisse und die hiermit korrespondierenden Mitwirkungspflichten der beaufsichtigten Stellen durch die bundesrechtlichen Vorschriften der §§ 474 ff. StPO verdrängt und damit eine Wahrnehmung der aufsichtsbehördlichen Befugnisse insbesondere den in § 479 StPO genannten Beschränkungen unterliegt.

Im Ergebnis ist diese Sichtweise jedoch abzulehnen. Zwar handelt es sich bei der Anforderung von Informationen und Unterlagen durch die Aufsichtsbehörde und die daraufhin erfolgende Zurverfügungstellung von Informationen mit personenbezogenem Inhalt durch den Verantwortlichen im technischen Sinne um eine Weitergabe personenbezogener Daten. Im rechtlichen Sinne liegt jedoch in diesen Fällen keine Übermittlung personenbezogener Daten vor, die an den Vorgaben der §§ 474 ff. StPO zu messen wäre. Die vereinzelt geäußerte gegenteilige Auffassung muss vor dem Hintergrund der heutigen Rechtslage als überholt bezeichnet werden. Zudem übersieht sie den Regelungsgrund der §§ 474 ff. StPO und verkennt die verfassungsrechtliche Herleitung und das Wesen der datenschutzrechtlichen Aufsicht.

*aa) Systematik*

Die insbesondere von *Kesten*[29] im Jahr 2002 publizierte Gegenauffassung wird insbesondere damit begründet, die §§ 474 ff. StPO würden als bundesgesetzliche Vorschriften den landesgesetzlich normierten Auskunfts- und Mitwirkungspflichten vorgehen. Aber selbst *Kesten* räumt in seinen Ausführungen ein: „Wenn der Bundesgesetzgeber will, dass der Landesdatenschutz die Ausführung von Bundesgesetzen überprüfen darf, regelt er das ausdrücklich."[30] Der heutige Gesetzgeber hat mit § 500 StPO ausdrücklich eine Datenschutzaufsicht im Ermittlungsverfahren vorgesehen und Art und Umfang der Befugnisse an den Landesgesetzgeber delegiert. Für die Anwendung der §§ 474 ff. StPO bleibt damit schon aus systematischen Gründen kein Raum.

---

25 *EuGH*, Urt. vom 9.3.2010 – C 518/07.

26 In § 16 BDSG (erster Teil) sind Befugnisse für den Bundebeauftragten für Datenschutz normiert, die jedoch hier keine Anwendung finden.

27 *Schwichtenberg*, in: Kühling/Buchner, DS-GVO/BDSG, § 68 Rn. 4.

28 BT-Drs. 19/4671, S. 71.

29 *Kesten,* SchlHA 2002, 228.

30 *Kesten,* SchlHA 2002, 228 (229).

*bb) Sinn und Zweck*

Die vorgenannte Gegenauffassung ist darüber hinaus aber vor allem auch aus dogmatischen Gründen abzulehnen. Die §§ 474 ff. StPO regeln nur die Zulässigkeit von Akteneinsicht und Auskünften aus Akten eines Strafverfahrens für sog. zweckumwandelnde, d.h. verfahrensexterne Zwecke.[31] Dementsprechend ist der Anwendungsbereich der §§ 474 ff. StPO bspw. schon nicht berührt, wenn es um die Vorlage von Akten an andere, im selben Verfahren mitwirkende Behörden und Gerichte oder an übergeordnete Behörden geht, da es in diesen Fällen an einer (rechtfertigungsbedürftigen) Zweckänderung fehlt.[32] Regelungsgrund der §§ 474 ff. StPO ist, dass jede Zweckumwandlung/-änderung wegen der damit einhergehenden Erweiterung der Datennutzung einen neuen eigenständigen Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) begründet, der einer verfassungsrechtlichen Rechtfertigung in Form eines Parlamentsgesetzes[33] bedarf.[34]

Demgegenüber erfolgt bei der datenschutzrechtlichen Aufsicht die Beauskunftung personenbezogener Daten nicht zu neuen, anderen Zwecken. Eine Zweckumwandlung/-änderung findet nicht statt. Vielmehr dient die datenschutzrechtliche Aufsicht gerade dazu zu überprüfen, ob die Datenverarbeitung der beaufsichtigten Stelle im Rahmen der ursprünglichen Zweckfestlegung erfolgt und ob sie diesem Zweck angemessen und erheblich ist. Sie unterscheidet sich organisatorisch und verfahrensrechtlich, nicht jedoch inhaltlich – gleichwohl aber thematisch auf datenschutzrechtliche Fragen beschränkt – von der Kontrolle, die auch die Gerichte ausüben.

Die aufsichtliche Kontrolle dient der Gewährleistung der Gesetzmäßigkeit der Verwaltung insgesamt. Sie muss wirksam und unabhängig[35] ausgestaltet sein und erstreckt sich auf den gesamten Prozess der Verarbeitung personenbezogener Daten inklusive der Gestaltung der Datenverarbeitung und der verwendeten Hilfsmittel.[36] Sie kompensiert auch das Rechtsschutzdefizit der betroffenen Personen (Beschuldigte, aber auch Opfer, Zeugen, andere Personen, die im Rahmen von strafprozessualen Ermittlungsmaßnahmen miterfasst werden), die wegen fehlender unmittelbarer Wahrnehmbarkeit und den sich hieraus ergebenden Rechtsschutzlücken, ihre Rechte auf Löschung, Berichtigung oder gerichtliche Überprüfung nicht selbst geltend machen können. Die datenschutzrechtliche Aufsicht flankiert die subjektivrechtliche Kontrolle durch die Gerichte objektivrechtlich.[37]

Die aufsichtliche Kontrolle gehört somit zu den Voraussetzungen einer verhältnismäßigen Ausgestaltung der Datenverarbeitung. Das Fehlen eines hinreichend wirksamen aufsichtsrechtlichen Kontrollregimes führt zu einer Unverhältnismäßigkeit und damit zu einer Verfassungswidrigkeit der entsprechenden Eingriffe.[38] Die Wahrnehmung der aufsichtlichen Befugnisse hat damit, anders wie in den Fällen der §§ 474 ff. StPO vorausgesetzt, keine eingriffsverstärkende, sondern ganz im Gegenteil eine den staatlichen Eingriff abmildernde und den Eingriff reduzierende Funktion und Wirkung. Eine Anwendung der Vorschriften der §§ 474 ff. StPO auf die Situation einer aufsichtlichen Kontrolle ist damit fernliegend.

Für den Bereich der Fach- und Rechtsaufsicht ist dies im Übrigen allgemein anerkannt und unbestritten.[39] Zum Ausdruck kommt dies z.B. auch in der RiStBV. Die Bestimmungen Nr. 183-189 RiStBV, die die gesetzlichen Vorschriften der §§ 474 ff. StPO konkretisieren, finden nach RiStBV 182 Nr. 2 keine Anwendung im Rahmen der Wahrnehmung von Aufsichts- und Kontrollbefugnissen anderer Stellen. Dies entspricht auch dem Willen des Gesetzgebers, der die Wahrnehmung von Aufsichts- und Kontrollbefugnissen nicht den Beschränkungen der §§ 474 ff. StPO unterwerfen wollte.[40] Als Ausdruck eines allgemeinen Rechtsgedankens stellt dies zudem § 7 Abs. 1 SDSG deklaratorisch klar, wonach eine Verarbeitung personenbezogener Daten durch öffentliche Stellen zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen keine Zweckänderung darstellt. Auch die Datenschutzaufsicht ist eine Aufsichts- und Kontrollinstanz im vorgenannten Sinne.

*cc) Eigene Auffassung*

Eine Anwendbarkeit der §§ 474 ff. StPO ist zudem mit dem Wesen einer Aufsicht im Allgemeinen und der datenschutzrechtlichen Aufsicht im Speziellen nicht vereinbar. Betrachtet man mit dem *BVerfG* die Existenz einer wirksamen, unabhängigen datenschutzrechtlichen Kontrolle[41] als notwendige Voraussetzung einer verhältnismäßigen Ausgestaltung staatlicher Befugnisse, wie sie gerade auch im strafprozessualen Ermittlungsverfahren existieren, und damit als verfassungsrechtliche Obliegenheit, wird schnell deutlich, dass eine Weitergabe personenbezogener Daten nicht an §§ 474 ff. und den dort genannten Einschränkungen gemessen werden kann. Denn die Vorschriften sehen anders als dies verfassungsrechtlich für eine wirksame Aufsicht geboten wäre, keine Übermittlungspflicht, sondern lediglich eine Übermittlungsbefugnis vor und stellen damit die Übermittlung ins Ermessen der Strafverfolgungsbehörde. Für die verfassungsrechtlich notwendige Aufsicht würde dies bedeuten, dass sie zur Wahrnehmung ihrer Aufgaben vom Goodwill der beaufsichtigten Stelle abhängig wäre. Mit dem Wesen und der Funktion einer Aufsicht ist dies schlichtweg nicht zu vereinbaren.

---

31 *VGH Mannheim*, NJW 2005, 234 (235); *LAG Hamm,* Urt. v. 10.7.2012 – 14 Sa 1711/10, Rn. 173 – juris; *Wittig*, in: BeckOK-StPO, 37. Ed (1.7.2020), § 474 Rn. 1; *Gieg*, in: KK-StPO, 8. Aufl. (2019), § 474 Rn. 1 m.w.N.

32 *Gieg*, in: KK-StPO, § 474 Rn. 1.

33 *BVerfG*, Stattgebender Kammerbeschluss v. 11.8.2009 – 2 BvR 941/08, Rn. 19. *VerfGH des Saarlandes*, Beschl. v. 28.8.2020 – Lv 15/19, S. 27 f.

34 *BVerfG*, Beschl. v. 18.12.2018 – 1 BvR 142/15, Rn. 162 ff.

35 *BVerfG*, Urt. v. 14.7.1999 – 1 BvR 2226/94; BVerfGE 100, 313 Rn. 171.

36 *BVerfG*, Urt. v. 19.5.2020 – 1 BvR 2835/17, Rn. 276.

37 *BVerfG*, Urt. v. 24.4.2013 – 1 BvR 1215/07; BVerfGE 133, 277 Rn. 207.

38 *BVerfG*, Urt. v. 24.4.2013 – 1 BvR 1215/07; BVerfGE 133, 277 Rn. 207.

39 *Gieg*, in: KK-StPO, § 474 Rn. 1; Radtke/*Hohmann*, StPO, 2011, § 474 Rn. 2; *Köhler*, in: Meyer-Goßner/Schmitt, StPO, 63. Aufl. (2020), § 474 Rn. 1.

40 BT-Drs. 14/1484, S. 25 f.

41 *BVerfG*, Urt. v. 14.7.1999 – 1 BvR 2226/94; BVerfGE 100, 313 Rn. 171.

*3. Adressaten aufsichtlicher Maßnahmen*

Die Ausübung der datenschutzrechtlichen Kontroll- und Aufsichtsbefugnisse erfolgt im Regelfall gegenüber dem Verantwortlichen/der verantwortlichen Stelle, kann aber auch gegenüber einem etwaigen Auftragsverarbeiter erfolgen (siehe die Erwähnung des Auftragsverarbeiters in der Formulierung der einzelnen Befugnisse in Art. 47 JI-RL). Die Umsetzung in § 20 SDSG unter Verweis auf die Befugnisse nach Art. 58 DSGVO hat diese Möglichkeit übernommen.

Verantwortlicher ist nach § 500 StPO i.V.m. § 46 Nr. 7 BDSG die Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dies ist jeweils im Einzelfall festzustellen. Soweit die Staatsanwaltschaft die Polizei mit konkreten Ermittlungsmaßnahmen beauftragt, spricht Vieles dafür, dass die Staatsanwaltschaft über die Zwecke und Mittel der Verarbeitung entscheidet. Wird die Polizei indes auf Grund ihrer aus § 163 StPO folgenden Kompetenz tätig, spricht Vieles dafür die Polizei als Verantwortlichen anzusehen. Sie wird in den Fällen des § 163 StPO ohne Anordnung der Staatsanwaltschaft tätig und entscheidet daher selbstständig über die Zwecke und Mittel der Verarbeitung personenbezogener Daten. Selbst wenn man die Polizei in diesen Fällen als Auftragsverarbeiterin der Staatsanwaltschaft i.S.d. § 62 BDSG ansehen wollte – was aus hiesiger Sicht fernliegend ist – würde dies in der Sache grundsätzlich nichts ändern, da Art. 47 JI-Richtlinie und § 20 SDSG ein aufsichtsbehördliches Tätigwerden auch gegenüber dem Auftragsverarbeiter gestatten. Wie bereits erwähnt ist dies auch verfassungsrechtlich geboten. Das *BVerfG* fordert, dass sich die datenschutzrechtliche Aufsicht auf den gesamten Prozess der Verarbeitung personenbezogener Daten inklusive der Gestaltung der Datenverarbeitung und der verwendeten (technischen und organisatorischen) Hilfsmittel erstrecken muss.[42]

Denkbar wäre zudem auch eine gemeinsame Verantwortlichkeit von Polizei und Staatsanwaltschaft i.S.d. § 63 BDSG anzunehmen. Aus der Rechtsprechung des *EuGH* folgt jedoch, dass auch im Rahmen einer gemeinsamen Verantwortlichkeit jeder Verantwortliche den Datenschutzvorschriften unterliegt[43] und gegen jeden Verantwortlichen vorgegangen werden kann.[44]

Werden die datenschutzrechtlichen Aufsichts- und Kontrollbefugnisse gegenüber der Polizei geltend gemacht, ist es zudem nicht erforderlich vorher die Staatsanwaltschaft zu beteiligen. Eine solche Notwendigkeit, die sich aus der Sachleitungsbefugnis der Staatsanwaltschaft ergeben soll, ist der datenschutzrechtlichen Aufsicht fremd und auch mit der Unabhängigkeit der datenschutzrechtlichen Aufsicht nicht zu vereinbaren. Die Sachleitungsbefugnis ist ein rein strafprozessuales Element, das die Leitung der **Ermittlungen** ganz in Hand der Staatsanwaltschaft verortet, aber keine Implikationen für die datenschutzrechtliche Verantwortlichkeit enthält.[45]

Die Notwendigkeit einer vorherigen Beteiligung der Staatsanwaltschaft würde auch die Wirksamkeit aufsichtsbehördlicher Maßnahmen beeinträchtigen, insbesondere bei unangekündigten Kontrollen oder solchen, die einer besonderen Eilbedürftigkeit geschuldet sind, und würde daher Zweifel an der Unabhängigkeit der Aufsichtsbehörde begründen. Für die Unabhängigkeit ist es erforderlich, dass die Aufsichtsbehörde „ihre Aufgaben ohne äußere Einflussnahme [wahrnehmen kann]“.[46] Wäre die Aufsichtsbehörde nun verpflichtet – insbesondere im Falle der Ausübung von Untersuchungsbefugnissen gegenüber der Polizei – vorher die Zustimmung der Staatsanwaltschaft einzuholen, bekäme die Staatsanwaltschaft einen unmittelbaren Einfluss auf die Durchführung der datenschutzrechtlichen Kontrolle. Im Extremfall könnte dies den Erfolg aufsichtsbehördlicher Maßnahmen vereiteln.

## III. Schlussfolgerungen

Aus den vorgenannten Ausführungen lassen sich Schlussfolgerungen für die Verfahrensweise bei datenschutzrechtlichen Kontrollen der Landesbeauftragten für Datenschutz in laufenden Ermittlungsverfahren ableiten. Hierbei ist zwischen Untersuchungsbefugnissen und Abhilfebefugnissen zu unterscheiden.

*1. Untersuchungsbefugnisse*

Die Untersuchungsbefugnisse ermöglichen es den jeweiligen Landesbeauftragten den relevanten Sachverhalt umfassend zu ermitteln. Sie sind Voraussetzung für eine tatsächliche Feststellung der konkret erfolgenden Datenverarbeitung und ermöglichen so erst eine datenschutzrechtliche Bewertung im Hinblick auf Art, Umfang und Angemessenheit der Verarbeitung. Eine Einschränkung der Untersuchungsbefugnisse sehen die europarechtlichen und verfassungsrechtlichen Vorgaben nicht vor.

Eine Zustimmungsbedürftigkeit der Staatsanwaltschaft bei der Wahrnehmung von Untersuchungsbefugnissen gegenüber der Polizei ist ebenso nicht vorgesehen und daher auch nicht erforderlich. Eine solche macht auch keinen Sinn, da wegen der Unanwendbarkeit der §§ 474 ff. StPO der Staatsanwaltschaft kein Spielraum verbleibt, nach einer eigenen Prüfung die Zurverfügungstellung personenbezogener Daten zu bejahen oder abzulehnen (gebundene Entscheidung) und würde folglich eine reine Formalie darstellen. Die jeweiligen landesrechtlichen Vorschriften sehen im Regelfall eine Unterstützungs**pflicht** vor und räumen weder der Polizei noch der Staatsanwaltschaft einen Ermessensspielraum ein.

---

42 *BVerfG*, Urt. v. 24.4.2013 – 1 BvR 1215/07; BVerfGE 133, 277 Rn. 207.
43 *EuGH*, Urt. v. 10.7.2018 – C 25/17, Rn. 65.
44 *EuGH*, Urt. v. 5.6.2018 – C 210/16.
45 *VG Hamburg*, Urt. v. 23.10.2019 – 17 K 203/19, S. 14.
46 *EuGH*, Urt. v. 9.3.2010 – C 518/07.

Dies schließt es selbstverständlich nicht aus, dass im Falle von angekündigten Kontrollen und solchen, die ohne Zeitnot erfolgen, im Wege der kollegialen Zusammenarbeit auch eine vorherige Inkenntnissetzung über die bevorstehende oder beabsichtigte Kontrolle durch die Landesbeauftragten für Datenschutz an die Staatsanwaltschaft erfolgt. Hierzu wäre es denkbar, dass zwischen den beiden Dienststellen eine entsprechende Vereinbarung geschlossen würde.

*2. Abhilfebefugnisse*

Bei den Abhilfebefugnissen hingegen stellt sich die Situation komplexer dar. Die Ausübung etwaiger aufsichtsbehördlicher Abhilfebefugnisse birgt immer die Gefahr, dass hierdurch das strafrechtliche Ermittlungsverfahren beeinträchtigt wird. Dies würde mit der Sachleitungsbefugnis der Staatsanwaltschaft kollidieren. Wenn auch die (europa)rechtlichen Rahmenbedingungen in diesen Fällen grundsätzlich die oben erwähnten Abhilfebefugnisse zur Verfügung stellen, so muss die konkrete Anwendung der gesetzlichen Vorschriften im Einzelfall diese Konfliktsituation im Rahmen der Ermessensausübung berücksichtigen. Dies gilt zum einen im Hinblick auf die Adressaten entsprechender Abhilfebefugnisse. Sinnvoll erscheint es, Abhilfemaßnahmen ausschließlich gegenüber dem Verantwortlichen, nicht jedoch gegenüber einem etwaigen Auftragsverarbeiter geltend zu machen. Entscheidender ist aber, dass sich die Auswahl der im konkreten Fall anzuwendenden Abhilfemaßnahmen, gerade auch im laufenden Ermittlungsverfahren, möglicherweise aus gegenläufigen strafprozessualen Interessen konkret auf die Abhilfebefugnisse/Mittel der Beanstandung und/oder Warnung beschränkt. Hierfür spricht unter anderem, dass eine möglicherweise datenschutzwidrige Datenverarbeitung im Ermittlungsverfahren nicht zwingend auch zu einem späteren Verwertungsverbot führt. Dies zu beurteilen ist ausschließlich Aufgabe der Gerichte. Hinzu kommt, dass zwar das *BVerfG* eine wirksame, unabhängige Rechtskontrolle administrativen Charakters voraussetzt, jedoch nicht verlangt, dass dieser Kontrollinstanz eine abschließende Entscheidungsbefugnis zukommt. Vielmehr soll es ausreichen, wenn ihr ein Beanstandungsrecht zugebilligt wird.[47] Gerade im strafrechtlichen Ermittlungsverfahren an deren Ende im Regelfall eine gerichtliche Überprüfung zwingend vorgesehen ist, bedarf es keiner abschließenden Entscheidungsbefugnis, die der gerichtlichen Entscheidung vorgreifen würde.

Dies gilt insbesondere soweit die datenschutzrechtliche Aufsicht sich auf ein konkretes Ermittlungsverfahren bezieht und Gegenstand der Aufsicht die konkrete Ermittlungsakte bzw. deren Inhalt ist. Ausreichend aber auch notwendig ist, dass die Datenschutzaufsicht die Zulässigkeit einer konkreten Ermittlungsmaßnahme aus datenschutzrechtlicher Sicht prüfen und bewerten kann. Werden hierbei Verstöße gegen datenschutzrechtliche Vorschriften festgestellt, so ist eine Beanstandung gegenüber der Fach- und Rechtsaufsichtsbehörde grundsätzlich ausreichend. Hierdurch wird die datenschutzrechtliche Bewertung aktenkundig und es kann dem datenschutzrechtlichen Verstoß durch die Fach- und Rechtsaufsicht begegnet werden bzw. er gegebenenfalls im späteren gerichtlichen Verfahren (inzidenter weise) überprüft werden.

Anders sieht dies in den Fällen der §§ 483-491 StPO aus. Die Vorschriften erlauben die Verarbeitung personenbezogener Daten (unter anderem auch) zu verfahrensübergreifenden Zwecken. Im Gegensatz zu den §§ 474-482 StPO, wo Zweckumwidmung und Übermittlungsvorschriften im Vordergrund stehen, ist Regelungsgegenstand hier die Voraussetzungen und Grenzen der elektronischen Speicherung und Nutzung personenbezogener Daten. Neben Strafverfahrensdateien nach § 483 StPO können danach auch Dateien zur Strafverfolgungsvorsorge (§ 484 StPO) sowie zur Vorgangsverwaltung (§ 485 StPO) betrieben werden. Die Vorschriften betreffen damit nicht nur die Datenverarbeitung für ein konkretes Ermittlungsverfahren, sondern auch den Betrieb von (verfahrensübergreifenden) Informationssystemen (Dateien), die sich aus unterschiedlichen Ermittlungsverfahren speisen (bspw. Mehrländer-Staatsanwaltschafts-Automation [MESTA] oder SIJUS-Straf-StA).[48] Eine immer größere Rolle spielen zudem neuere Formen der Verarbeitung insbesondere von Massendaten. Neben Datenanalyseinstrumenten handelt es sich dabei auch um Programme, die dem Prinzip des Data Mining folgen oder sogar Big Data-Analysen vornehmen können.[49]

Anders als die konkrete Ermittlungsakte finden zwar die (Auswerte)Ergebnisse solcher Systeme, nicht aber die Systeme selbst Eingang in das gerichtliche Verfahren. Deren Betrieb und Verarbeitung endet auch nicht mit dem Abschluss des Ermittlungsverfahrens. Eine zwingende gerichtliche Überprüfung findet für diese Systeme nicht statt. Gleichzeitig spielen bei diesen Informationssystemen in größerem Maße als bei der Ermittlungsakte auch die Umsetzung technischer und organisatorischer Maßnahmen eine erhebliche Rolle. Hier besteht ein unverkennbarer Bedarf nach einer wirksamen datenschutzrechtlichen Kontrolle, um den Betrieb dieser Systeme kritisch begleiten zu können. Aus datenschutzrechtlicher Sicht reicht das Mittel der Beanstandung in diesen Fällen jedoch nicht aus, sondern es bedarf wirksamer Abhilfebefugnisse durch die Landesbeauftragte für Datenschutz, die es ihr letztlich auch ermöglichen, bei Fehlentwicklungen regulativ eingreifen zu können.

Gleichwohl wird aber auch hier im konkreten Fall der Aufsicht ein zweistufiges Verfahren, mittels einer vorherigen, erfolglosen Beanstandung angezeigt und im Regelfall auch ausreichend sein. Eine Bindungswirkung folgt für die beaufsichtigte Stelle bei festgestellten und begründeten Defiziten bereits unmittelbar aus dem Grundsatz der Gesetzmäßigkeit der Verwaltung. Es bedarf hierzu im Regelfall keiner regelnden Konkretisierung der gesetzlichen

[47] *BVerfG*, Urt. v. 19.5.2020 – 1 BvR 2835/17, Rn. 276.
[48] *Singelnstein*, in: MüKo-StPO, 2019, vor § 483 Rn. 3.
[49] *Singelnstein*, in: MüKo-StPO, vor § 483 Rn. 16.

Pflichten in Form eines exekutiven Handelns durch eine andere staatliche Stelle. In Ausnahmefällen ist aber auch dies möglich und angezeigt, wenn nämlich die beaufsichtigte Stelle auf die Beanstandung nicht oder nicht angemessen reagiert.