LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

STELLUNGNAHME
18/582

A14

Anhörung von Sachverständigen des Rechtsausschusses

Prof. Dr. Bettina Schöndorf-Haubold
Professorin für Öffentliches Recht
Justus-Liebig-Universität Gießen

Stellungnahme zum Fragenkatalog

„Löschung von Daten als Ergebnis staatsanwaltschaftlicher Ermittlungen unter Betrachtung des Urteils des Bundesverfassungsgerichts“
Vorlage 18/1027

Anhörung des Rechtsausschusses am Montag, dem 5. Juni 2023

Fragenkatalog: Beantwortung der Fragen 1. – 6.

- **1. Wie bewerten die Sachverständigen unter Berücksichtigung der Hinweise der Landesdatenschutzbeauftragten im Bericht von 2022 auf den Seiten 52-55, dass Daten von Bürgerinnen und Bürgern nicht gelöscht werden, die eigentlich zu löschen wären?**

Eine Nichtlöschung von personenbezogenen Daten trotz Löschungspflicht wirft zunächst Fragen in Bezug auf ihre Vereinbarkeit mit Grundrechten auf (a). Darüber hinaus ist zu prüfen, wann und inwiefern das Unionsrecht eine Löschung personenbezogener Daten gebietet (b), so dass eine entsprechende Praxis der Sicherheitsbehörden auch einen Verstoß gegen Sekundärrecht zur Folge haben könnte (c). Der objektiven Verpflichtung zur Datenlöschung entspricht ein einfachrechtlich ausgestalteter Anspruch auf Datenlöschung (d) wie auch ein Recht auf gerichtlichen Rechtsschutz (e). Neben den primär für die Datenverarbeitung und damit auch für die Löschung Verantwortlichen kommt insbesondere auch den Datenschutzbeauftragten die Aufgabe der wirksamen Durchsetzung der betreffenden Bestimmungen zu (f). Mit der dergestalt differenzierten Beantwortung der ersten Frage soll zugleich der rechtliche Hintergrund für alle weiteren Fragen erläutert werden.

a) Grundrechtlicher Rahmen

Die gesetzlich anzuordnende Verpflichtung zur Löschung von Daten stellt eine zentrale flankierende Voraussetzung für die Verhältnismäßigkeit der Datenerhebung, -nutzung und –speicherung dar.[1] Ein im Rahmen einer gesetzlichen Anordnung verfassungsrechtlich

[1] Vgl. grundlegend bereits BVerfGE 65, 1 (46 - Volkszählung): „Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich.“; BVerfGE 100, 313 (362 – dort in Bezug auf Art. 10 GG): „Schließlich müssen die erlangten Daten […] vernichtet werden, sobald sie für die festgelegten Zwecke oder den gerichtlichen Rechtsschutz nicht mehr erforderlich sind.“; BVerfGE 141, 220 (285 Rn. 144 –

zulässiger Eingriff in das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[2] (bzw. ggf. weitere speziellere Grundrechte[3]) verliert seine Rechtfertigung, wenn die Löschung trotz einer bestehenden gesetzlichen Verpflichtung nicht vorgenommen wird. Die Nichtlöschung trotz entsprechender Verpflichtung führt damit zu einer Grundrechtsverletzung und stellt einen fortdauernden Eingriff in das Recht auf informationelle Selbstbestimmung dar.[4]

Eine Heilung einer verfassungswidrigen Nichtlöschung durch Zweckänderung kommt ebenfalls nicht in Betracht. Auch die spezifischen Anforderungen, die das Bundesverfassungsgericht in ständiger Rechtsprechung an eine Zweckänderung der Datennutzung stellt,[5] setzen eine rechtmäßige und verfassungskonforme Datenerhebung und Datenspeicherung voraus. Insbesondere dient der Grundsatz der hypothetischen Datenneuerhebung in den Fällen einer Zweckänderung nicht dazu, eine ursprünglich fehlerhafte und damit verfassungswidrige Datenspeicherung zu heilen.[6]

Das BVerfG geht in st. Rspr. davon aus: „Die Begrenzung der Datenverwendung auf bestimmte Zwecke muss auch für die Verwendung der Daten nach deren Abruf und Übermittlung an die abrufenden Behörden sichergestellt und verfahrensmäßig flankiert werden. Insoweit ist gesetzlich zu gewährleisten, dass die Daten nach Übermittlung unverzüglich ausgewertet werden und, sofern sie für die Erhebungszwecke unerheblich sind, gelöscht werden […]. Im Übrigen ist vorzusehen, dass die Daten vernichtet werden, sobald sie für

---

BKAG): „Zu den übergreifenden Verhältnismäßigkeitsanforderungen gehört auch die Regelung von Löschungspflichten […]. Mit ihnen ist sicherzustellen, dass eine Verwendung personenbezogener Daten auf die die Datenverarbeitung rechtfertigenden Zwecke begrenzt bleibt und nach deren Erledigung nicht mehr möglich ist."; BVerfGE 150, 244 (285 Rn. 101 – automatisierte Kennzeichenerfassung): tragfähige Regelungen zur Datenlöschung; ähnlich BVerfGE 156, 11 (46 Rn. 89 – ATDG II); stRspr. Zur Normierung von Löschpflichten als Voraussetzung für die Verhältnismäßigkeit polizeilicher Datenerhebung s. auch *Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 301.

[2] Zur Entwicklung in der Rechtsprechung des BVerfG s. *Schöndorf-Haubold*, Das Recht auf Achtung des Privatlebens, Grundrechtsschutz in der Informationsgesellschaft, 2020, S. 49 ff.

[3] Neben dem ebenfalls aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (BVerfGE 120, 274 (302 ff.)) kommen auch speziellere Grundrechte wie Art. 10 und Art. 13 GG in Abhängigkeit von der Qualität und den Erhebungsvoraussetzungen der gespeicherten Daten in Betracht. Die grundlegenden Voraussetzungen des datenschutzrechtlichen Grundrechtsschutzes unterscheiden sich allerdings nicht.

[4] Vgl. KK-StPO/*Gieg*, 9. Aufl. 2023, StPO § 489 Rn. 2. Hiervon sind Fälle zu unterscheiden, in denen die Rechtfertigung der Speicherung umstritten ist, im Ergebnis aber etwa im Rahmen der elektronischen Vorgangsbearbeitung ausschließlich zur Dokumentation für zulässig erachtet wird. Hierzu OVG Lüneburg NVwZ-RR 2020, 973 (kein Löschungsanspruch); BVerwG v. 21.1.2019, 6 B 139/18, Juris.

[5] S. zusammenfassend BVerfG NJW 2023, 1169 (1199 – Rn. 51 ff.): Grundsatz der Zweckbindung, Voraussetzungen der zweckwahrenden bzw. zweckändernden Weiternutzung; BVerfGE 141, 220 (BKA-Entscheidung Rn. 276 ff.).

[6] Zur umstrittenen Frage, ob und wann sich aus dem datenschutzrechtlichen Grundrechtsverstoß ein strafprozessuales Verwertungsverbot ergibt, s. *Singelnstein*, Folgen des neuen Datenschutzrechts für die Praxis des Strafverfahrens und die Beweisverbotslehre, NStZ 2020, S. 639 ff. (insb. S. 643 ff., dort allerdings zu einer rechtswidrigen Erhebung der Daten); s. auch *Cordes/Reichling*, Grenzen der Durchsicht von Papieren und elektronischen Speichermedien gemäß § 110 StPO und Rechtsfolgen von Verstößen, NStZ 2022, S. 712 (716): bei einer schwerwiegenden Rechtsmissachtung (dort des Richtervorbehalts) soll es jedenfalls auch nicht auf einen hypothetisch rechtmäßigen Ermittlungsverlauf ankommen.

die festgelegten Zwecke nicht mehr erforderlich sind, und dass hierüber ein Protokoll gefertigt wird […]."[7]

In den Fällen, in denen – über die Fragestellung hinaus – ein sog. Restverdacht die weitere Speicherung der Daten trotz eines Freispruchs oder in Fällen einer Verfahrenseinstellung tatsächlich rechtfertigt, begegnet dies ggf. mit Blick auf die Unschuldsvermutung grundrechtlichen und rechtsstaatlichen Bedenken.[8]

Neben Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG sind auch die Grundrechte der Europäischen Grundrechtecharta, insb. Art. 7 und 8 EU-GRC, Art. 16 Abs. 1 AEUV sowie Art. 8 EMRK[9] zu beachten. Landesverfassungsrechtlich sieht auch Art. 4 Abs. 2 VerfNRW einen ausdrücklichen Anspruch auf Schutz der personenbezogenen Daten vor**.** Auf der Grundlage der Rechtsprechung sowohl des BVerfG als auch des EuGH kann trotz Grundrechtspluralität auf der Basis der Europäischen Grundrechtecharta wie auch der EMRK im Grundsatz von einem übergreifenden gemeinsamen Grundrechtsniveau und damit von einer weitgehenden Parallelität der grundrechtlichen Gewährleistungen ausgegangen werden.[10] Zusätzliche Verpflichtungen – insbesondere auch für den Umgang mit strafverfahrensrechtlichen Daten – können sich darüber hinaus aus Art. 19 Abs. 4 GG, Art. 47 EU-GRC sowie aus Art. 6 Abs. 2 EMRK[11] ergeben.

---

[7] BVerfGE 125, 260 (332 f. - Vorratsdatenspeicherung) mit Verweis auf BVerfGE 100, 313 (362, 387 f.) und BVerfGE 113, 29 (58).

[8] S. dazu *Arzt*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 1280 ff m.w.N.; EGMR 48144/09 (C./Deutschland), NJW 2016, 3225; BVerfG NJW 2002, 3231; s. auch die Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Neustrukturierung des BKAG, BR-Drs. 109/17 (Regierungsentwurf) und BT-Drs. 18/11163 (Fraktionsentwurf), vom 10.3.2017, S. 21 f. (mit Verweis auf EGMR NJOZ 2010, 696 Marper): „Der verbleibende Tatverdacht kann verschieden stark ausgeprägt sein, was nicht zuletzt die im Bereich der StPO vorgesehenen und anerkannten verschiedenen Arten des Tatverdachts belegen. Insbesondere muss die speichernde Stelle deshalb die Gründe für den fortbestehenden Tatverdacht und für dessen Gewicht bzw. den verbleibenden Verdachtsgrad besonders darlegen. Wie Ergebnisse datenschutzrechtlicher Kontrollen gezeigt haben, liegen oftmals nicht einmal Rückmeldungen zum Verfahrensausgang vor. Unabhängig davon haben sich – unabhängig von der Frage des bestehenden Restverdachts – teilweise erhebliche Dokumentationsdefizite hinsichtlich der Negativprognose gezeigt (so die Ergebnisse der Kontrolle der FDR in mehreren Bundesländern und im Bereich der Zollfahndung). Bei datenschutzrechtlichen Kontrollen habe ich trotz der Rechtsprechung des BVerfG und des EGMR – abgesehen von gerichtlich geprüften Fällen der DNA-Analyse – noch keinen Fall gefunden, in dem die datenverarbeitende Stelle sich mit dieser Frage befasst und dies dokumentiert hatte."

[9] S. z.B. EGMR v. 25.5.2021, 35252/08 (Centrum för Rättvisa / Schweden), NVwZ-Beilage 2021, 30 (40 Rn. 339 ff.): Prüfung der praktischen Anwendung der Löschregeln sowie deren effektive Kontrolle durch die Aufsichtsbehörden durch den EGMR in Fällen der geheimen Massenüberwachung der elektronischen Kommunikation; ähnlich EGMR v. 25.5.2021, 58170/13 ua. (Big Brother Watch / UK), NVwZ-Beil. 1/2021, 11 (15 ff. Rn. 335 ff.) ebenfalls zu Massenüberwachung.

[10] Vgl. nur BVerfGE 152, 152 (175 f. Rn. 55 ff. – Recht auf Vergessen I): „Vermutung", „dass durch eine Prüfung [unionsrechtlich nicht voll determinierten innerstaatlichen Rechts] am Maßstab der Grundrechte des Grundgesetzes das Schutzniveau der Charta, wie sie vom Europäischen Gerichtshof ausgelegt wird, in der Regel mitgewährleistet ist". Konsequent prüft das BVerfG unionsrechtlich vollständig determiniertes nationales Recht am Maßstab der Unionsgrundrechte, d.h. insb. am Maßstab der Europäischen Grundrechtecharta; BVerfGE 152, 216 (Recht auf Vergessen II).

[11] EGMR NJOZ 2010, 696 (700 ff. Rn. 103 f., 122 ff.).

b) Anforderungen der JI-Richtlinie

Einen unionsrechtlichen Mindeststandard, der aufgrund des Anwendungsvorrangs des EU-Rechts ebenfalls zu berücksichtigen ist, legt die JI-Richtlinie[12] fest, deren innerstaatliche Anwendung umgekehrt eine verfassungsrechtliche Kontrolle am Maßstab der Grundrechte des GG nicht ausschließt, da von ihr keine vollständige unionsrechtliche Determinierung ausgeht.[13]

Im Anwendungsbereich der JI-Richtlinie[14] stellt eine fortwährende Datenspeicherung trotz Bestehens einer Löschpflicht durch mitgliedstaatliche Behörden einen Sekundärrechtsverstoß dar, der ggf. zu einer Beanstandung durch die EU-Kommission und in der Konsequenz auch zu einem Vertragsverletzungsverfahren führen kann.[15] Auch die Nichtanwendung richtlinienkonformen nationalen Rechts kann einen Verstoß gegen die Richtlinie begründen. Ob bereits die Fehlanwendung der Richtlinie im Einzelfall oder erst eine verfestigte Verwaltungspraxis eine Vertragsverletzung darstellt,[16] spielt angesichts der von der Datenschutzbeauftragten festgestellten Verstöße im vorliegenden Fall keine Rolle.

Nach Art. 4 Abs. 1 d) und e) JI-RL gehört es zu den Grundsätzen der Datenverarbeitung, dass „personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden“ und personenbezogene Daten allgemein „nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht“. Gemäß Art. 5 JI-RL sehen die Mitgliedstaaten vor, „dass für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen sind. Durch verfahrensrechtliche Vorkehrungen ist sicherzustellen, dass diese Fristen eingehalten werden.“[17]

Art. 16 Abs. 2 JI-RL verpflichtet die Mitgliedstaaten ausdrücklich dazu, vom Verantwortlichen zu verlangen, personenbezogene Daten unverzüglich zu löschen“ und vorzusehen, „dass die betroffene Person das Recht hat, von dem Verantwortlichen die Löschung von

---

[12] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. EU 2016 Nr. L 119/89.

[13] S. nur BVerfGE 158, 170 (183 Rn. 23 m.w.N. – IT-Sicherheitslücken); grundlegend BVerfG (Fn. 10).

[14] Zum Anwendungsbereich s. Art. 1 und 2 JI-RL (Fn. 12); ferner *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 403 ff., 455 ff.

[15] Vgl. den 31. Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit (für das Jahr 2022) des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, BT Drs. 20/6000, S. 47 f. mit Verweis auf die Mitteilung der Kommission an das Europäische Parlament und den Rat „Erster Bericht über die Anwendung und Wirkungsweise der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei der Strafverfolgung)“ COM(2022) 364 final v. 25.7.2022.

[16] Hierzu *Karpenstein*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der EU, Art. 258 AEUV Rn. 63 f. mwN. (Stand: EL 65 August 2018).

[17] Art. 13 Abs. 1 c) und Art. 14 d) JI-RL schließen Informationen zu Löschungsrechten in die von den Verantwortlichen zur Verfügung zu stellenden Informationen bzw. das Auskunftsrecht der betroffenen Person ein. Art. 13 Abs. 3 und Art. 15 Abs. 1 JI-RL sehen während laufender Verfahren sowie zu Zwecken der Gefahrenabwehr und Strafverfolgung allerdings Ausnahmen von dieser Unterrichtungspflicht vor.

sie betreffenden personenbezogenen Daten unverzüglich zu verlangen, wenn die Verarbeitung gegen die nach den Artikeln 4, 8 und 10 erlassenen Vorschriften verstößt oder wenn die personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen, der der Verantwortliche unterliegt."

Eine unverzügliche Benachrichtigung des Betroffenen im Falle eines Verstoßes gegen Verpflichtungen aus der Richtlinie sieht Art. 31 Abs. 1 JI-RL nur vor, „wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat." Einer unverzüglichen Meldung gegenüber der Aufsichtsbehörde bedarf es demgegenüber nach Art. 30 Abs. 1 JI-RL bereits bei einem „Risiko für die Rechte und Freiheiten natürlicher Personen".

Es obliegt der Aufsichtsbehörde nach Art. 46 Abs. 1 a) JI-RL, „die Anwendung der nach dieser Richtlinie erlassenen Vorschriften sowie deren Durchführungsvorschriften" zu überwachen und durchzusetzen. Hierzu muss die Aufsichtsbehörde vom jeweiligen Mitgliedstaat durch Rechtsvorschriften mit „wirksamen Überwachungsbefugnissen" ausgestattet werden. Sie muss nach Art. 47 Abs. 2 JI-RL außerdem „über wirksame Abhilfebefugnisse wie etwa die beispielhaft genannten verfügen, die es ihr gestatten, […] c) den Verantwortlichen […] anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in Einklang zu bringen, insbesondere durch die Anordnung der Berichtigung oder Löschung personenbezogener Daten […]".

Im Rahmen der jeweiligen Gesetzgebungskompetenzen sind sowohl der Bundes- als auch die Landesgesetzgeber zur Umsetzung dieser Bestimmungen verpflichtet; allen staatlichen Behörden obliegt sodann die richtlinienkonforme Anwendung des nationalen Rechts.

c) Vereinbarkeit mit der JI-Richtlinie: Umsetzung im Bundes- und Landesrecht

Da die Gesetzgebungskompetenz für das repressive Strafverfahrens- und das präventive Polizeirecht in Deutschland auseinanderfallen, sind Bundes- und Landesgesetzgeber gleichermaßen zur Umsetzung der JI-Richtlinie aufgerufen.

- **Bundesrechtliches Strafverfahrensrecht:**

Der Bundesgesetzgeber ist den Verpflichtungen der JI-Richtlinie für den Bereich des Strafverfahrensrechts insbesondere mit der Änderung der StPO von 2019[18] und der Novellierung des BDSG von 2017 nachgekommen, die grundsätzlich ergänzend nebeneinander anzuwenden sind.[19]

Nach § 47 BDSG müssen personenbezogene Daten insbesondere auf rechtmäßige Weise, für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden und dürfen

[18] Art. 1 des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 v. 20.11.2019, BGBl I 1724.

[19] Vgl. § 500 StPO sowie Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679, BT Drs. 19/4671, S. 44.

„nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht".[20]

Pflichten zur Löschung von Daten ergeben sich neben einer Reihe spezifischer Tatbestände[21] insb. aus § 489 StPO und § 75 Abs. 2 BDSG[22].

Nach § 489 Abs. 1 StPO „sind, unbeschadet der anderen, in § 75 Abs. 2 BDSG genannten Gründe für die Pflicht zur Löschung,

1. die nach § 483 gespeicherten Daten mit der Erledigung des Verfahrens, soweit ihre Speicherung nicht nach den §§ 484 und 485 zulässig ist,

2. die nach § 484 gespeicherten Daten, soweit die dortigen Voraussetzungen nicht mehr vorliegen und ihre Speicherung nicht nach § 485 zulässig ist, und

3. die nach § 485 gespeicherten Daten, sobald ihre Speicherung zur Vorgangsverwaltung nicht mehr erforderlich ist" zu löschen.[23]

§ 483 StPO erlaubt eine Speicherung personenbezogener Daten in Dateisystemen für die Zwecke eines konkreten Strafverfahrens, ihre Verwendung in anderen Strafverfahren und die Speicherung in polizeilichen Misch-Dateien mit gemischter repressiv-präventiver Funktion.[24] § 484 StPO gestattet die Speicherung eines Basisdatensatzes in einem Aktenhinweissystem zu Zwecken späterer Strafverfolgung[25] sowie die Speicherung weiterer personenbezogener Daten potentieller Wiederholungstäter bei Vorliegen eines (jeweils positiv festzustellenden) Restverdachts.[26] Demgegenüber richtet sich die Verarbeitung personenbezogener Daten – und damit sowohl Speicherung als auch Löschung – für die Zwecke künftiger Strafverfahren bei der und durch die Polizei gemäß § 484 Abs. 4 StPO nach

[20] Anforderungen an eine Zweckänderung enthalten § 479 Abs. 2 i.V.m. § 161 Abs. 3 StPO; s. dazu ausführlich KK-StPO/*Weingarten*, 9. Aufl. 2023, StPO § 161 Rn. 35 ff. auch zum Grundsatz der hypothetischen Datenneuerhebung und zum sog. Doppeltürmodell.

[21] Vgl. die Aufzählung im Gesetzentwurf der Bundesregierung (Fn. 19), BT Drs. 19/4671, S. 44

[22] Zur nur eingeschränkten Anwendung von § 58 Abs. 3 BDSG s. § 161 II StPO und § 489 Abs. 6 StPO. Zu Löschpflichten als Löschungspflicht als „zwingende Vorgabe bzw. Klarstellung von verfassungsrechtlichen Selbstverständlichkeiten" *Roggenkamp*, in: Specht/Manz (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 21 Rn. 94.

[23] Als Erledigung des Verfahrens gilt nach § 489 Abs. 2 „die Erledigung bei der Staatsanwaltschaft oder, sofern die öffentliche Klage erhoben wurde, bei Gericht. Ist eine Strafe oder eine sonstige Sanktion angeordnet worden, so ist der Abschluss der Vollstreckung oder der Erlass maßgeblich. Wird das Verfahren eingestellt und hindert die Einstellung die Wiederaufnahme der Verfolgung nicht, so ist das Verfahren mit Eintritt der Verjährung als erledigt anzusehen."

[24] Kritisch zu letzterem in Bezug auf die Verwischung der Grenzen zwischen Gefahrenabwehr und Strafverfolgung KK-StPO/*Gieg*, 9. Aufl. 2023, StPO § 483 Rn. 5 mwN. u.a. auf BVerwGE 137, 113 ff. = NJW 2011, 405: „Aus Gründen der Rechtssicherheit wäre deshalb eine Anpassung der Begrifflichkeiten in § 170, Nr. 88 RiStBV, § 8 Abs. 3 BKAG und § 484 Abs. 2 S. 2 mit dem Ziel nützlich, die Folgen der Einstellung eines strafrechtlichen Ermittlungsverfahrens für die Befugnis zur Datenspeicherung aus Gründen der vorbeugenden Verbrechensbekämpfung oder der Strafverfolgungsvorsorge normklarer zu gestalten" (Zitat bei *Gieg*).

[25] Kritisch hierzu KK-StPO/*Gieg*, 9. Aufl. 2023, StPO § 484 Rn. 2 mwN.

[26] BeckOK StPO/*Wittig*, 47. Ed. 1.4.2023, StPO § 484 Rn. 3 ff.; dort auch zum Fehlen einer Verordnung iSv § 484 Abs. 3 StPO.

den jeweiligen Polizeigesetzen. Im Rahmen der sog. Vorgangsverwaltung zur verwaltungsmäßigen Archivierung gespeicherte Daten dürfen gemäß § 485 StPO gespeichert und verarbeitet werden, solange dies für die Vorgangsverwaltung erforderlich ist.[27]

Entfällt die Rechtfertigung für die Speicherung, folgt hieraus grundsätzlich eine objektive Pflicht zur Löschung der betreffenden Daten sowie ein subjektiv-rechtlicher Anspruch des Betroffenen auf ebendiese Löschung.[28] Allein technische Gründe wie die systembedingte Unmöglichkeit einer Löschung einzelner Daten vermögen die weitere Speicherung nicht zu rechtfertigen, da „die Anforderungen an die technische Datenverarbeitung nach BVerfG den Anforderungen des Grundrechts auf informationelle Selbstbestimmung zu genügen [haben] und nicht umgekehrt".[29]

§ 75 Abs. 2 BDSG bestimmt darüber hinaus generell, dass der jeweilige Verantwortliche personenbezogene Daten unverzüglich zu löschen hat, „wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist." Die Norm ist neben den bereichsspezifischen Sonderregelungen der StPO anwendbar und begründet eigenständige Pflichten. § 75 Abs. 3 StPO sieht Ausnahmen vor, die im Rahmen der Löschungspflichten nach StPO gemäß § 161 Abs. 2 StPO vor allem bei besonders eingriffsintensiven Maßnahmen nicht zur Anwendung kommen.[30]

Die rechtliche Verpflichtung zur Löschung besteht kraft gesetzlicher Anordnung und setzt keinen Antrag der/des Betroffenen voraus. Umgekehrt verpflichtet sie die Datenverantwortlichen dazu, „Löschungsverpflichtungen **selbständig und laufend** auf ihr Bestehen und Nachkommen zu überprüfen".[31]

- **Landesrechtliches Polizeirecht:**

Auch die landesrechtlichen Regelungen des Polizeirechts sehen die Löschung der entsprechenden Daten in den polizeilichen Datenbanken in Umsetzung der JI-Richtlinie vor.[32] Aufgrund der entsprechenden Verweisungen in der StPO gelten die polizeirechtlichen Regelungen auch für sog. Mischdateien, in denen sowohl präventiv als auch repressiv erhobene Daten gespeichert werden (s.o.).

---

[27] Vgl. hierzu KK-StPO/Gieg, 9. Aufl. 2023, StPO § 485 Rn. 1 f. auch in Bezug auf fehlende ausdrückliche Speicherfristen und die gleichwohl bestehende Pflicht zur Löschung bei Wegfall der „Erforderlichkeit" der Speicherung.
[28] In Bezug auf § 484 StPO KK-StPO/*Gieg*, 9. Aufl. 2023, StPO § 484 Rn. 3.
[29] BVerfG Beschl. v. 13.5.2015 – 1 BvR 99/11, BeckRS 2015, 52585.
[30] Ob sich allein damit ein nur begrenzter Anwendungsbereich der Norm prognostizieren lässt, ist zu bezweifeln. So aber Gesetzentwurf der Bundesregierung (Fn. 19), BT Drs. 19/4671, S. 45. Insbesondere kann aus dem Fehlen ausdrücklicher Beweisverwertungsverbote weder auf den Wegfall einer Löschungspflicht noch auf eine Rechtfertigung weiterer Speicherung geschlossen werden. Kritisch zur Richtlinienkonformität von § 58 Abs. 3 BDSG BeckOK DatenschutzR/*Burghardt/Reinbacher*, 43. Ed. 1.8.2022, BDSG § 75 Rn. 4.
[31] *Johannes/Weinhold*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl., § 75 Rn. 24 f. (Hervorhebung im Original).
[32] Vgl. das Gesetz zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU – NRWDSAnpUG-EU)

Grundsätzlich gilt nach § 22 PolG NRW, dass rechtmäßig erlangte personenbezogene Daten (nur) so lange in Dateisystemen und Akten gespeichert werden können, wie dies zur polizeilichen Aufgabenerfüllung, zur zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist (Abs. 1). Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken; die Erforderlichkeit muss zu bestimmten festgesetzten Prüfungsterminen überprüft werden, die bestimmte Höchstfristen nicht überschreiten dürfen (Abs. 2). Im Falle eines rechtskräftigen Freispruchs, der unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens oder der nicht nur vorläufigen Einstellung des Verfahrens ist die Speicherung „unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat. Sollte eine Speicherung wegen eines Restverdachts einer Straftat weiterhin zulässig sein, ist dessen Gewicht und der Grad des Verdachts zu dokumentieren“ (§ 22 Abs. 3 PolG NRW).

Nach § 32 Abs. 1 PolG NRW sind personenbezogene Daten nach Maßgabe des § 54 i.V.m. § 50 Abs. 3 bis 5 DSG NRW zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken und darüber hinaus auch dann zu löschen, wenn dies durch das PolG NRW bestimmt ist, die Speicherung unzulässig ist oder bei einer Prüfung der Wegfall der Erforderlichkeit festgestellt wird. In diesem Fall (auch bei Wegfall eines Straftatverdachts) sind nach § 32 Abs. 1 S. 3 PolG NRW die in Dateien suchfähig gespeicherten Daten zu löschen sowie die zu der Person suchfähig angelegten Akten zu vernichten.[33]

In Ergänzung zu den polizeirechtlichen Bestimmungen normiert das DSG NRW allgemeine Grundsätze für die Verarbeitung personenbezogener Daten (§ 37 DSG NRW)[34] wie auch Rechte und Ansprüche betroffener Personen (§§ 47 ff. DSG NRW) und Pflichten der Datenverantwortlichen (§§ 52 ff. DSG NRW): Nach § 37 Nr. 4 und 5 DSG NRW sind Daten, „die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind“, unverzüglich zu löschen oder zu berichtigen und Daten insgesamt „nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht“. § 50 Abs. 2 DSG NRW räumt den Betroffenen ein § 58 Abs. 2 BDSG entsprechendes Löschungsrecht ein. § 54 Abs. 2 DSG NRW verpflichtet den Datenverantwortlichen auch ungeachtet individueller Ansprüche zur unverzüglichen Löschung entsprechend § 75 Abs. 2 BDSG.

Die entsprechenden Normen dienen damit sowohl der Umsetzung der sekundärrechtlichen Vorgaben der JI-Richtlinie als auch der verfahrensrechtlichen Anforderungen der Rechtsprechung des Bundesverfassungsgerichts zur Gewährleistung der Verhältnismäßigkeit von Eingriffen in das Recht auf informationelle Selbstbestimmung. Eine Nichtan-

[33] Zu den Voraussetzungen und Anforderungen an die Löschung s. BeckOK PolR NRW/Ogorek, 25. Ed. 15.4.2023, PolG NRW § 32 Rn. 15 ff.

[34] Insb. Rechtmäßigkeit der Verarbeitung, Zweckbindung und Datensparsamkeit.

wendung oder fehlerhafte Anwendung dieser Normen durch die StA und die Polizeibehörden führt daher zu einer Verletzung der JI-Richtlinie wie auch zu ungerechtfertigten Eingriffen in Grundrechte.

d) Löschungsanspruch

Konsequenz des Verstoßes gegen einfaches Recht und des sich hieraus ergebenden Grundrechtsverstoßes ist ein subjektiv-rechtlicher Anspruch auf Löschung der betreffenden Daten, der gegebenenfalls auch gerichtlich durchgesetzt werden kann. Sofern ein solcher Anspruch nicht einfachrechtlich ausdrücklich normiert ist, ist er durch entsprechende Auslegung des objektiven Rechts zu ermitteln.[35] In jedem Fall folgt aus den allgemeinen Grundsätzen für die Verarbeitung personenbezogener Daten, insbesondere den Grundsätzen der Datenminimierung, der Zweckbindung, der Erforderlichkeit und der Verhältnismäßigkeit, dass die Datenverantwortlichen eine mögliche Löschung nicht allein mit dem Ablauf von Speicher- oder Prüffristen ausschließen dürfen, sondern in regelmäßigen Abständen bzw. auf Antrag auch die Erforderlichkeit der weiteren Speicherung im Einzelfall prüfen müssen.[36]

Für Daten, die bei der Staatsanwaltschaft gespeichert sind, ergibt sich dieser Anspruch aus § 500 Abs. 1 StPO i.V.m. §§ 75 Abs. 2, 58 Abs. 2 BDSG bzw. i.V.m.. den besonderen Lösch-Tatbeständen des § 489 Abs. 1 und Abs. 2 StPO. [37] Nach § 58 Abs. 2 BDSG hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder dies zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

Auch die Bestimmungen der landesrechtlichen Datenschutzgesetze sehen entsprechende Löschungsansprüche wie in § 50 DSG NRW oder § 53 HDSIG zum Teil wortgleich zu § 58 Abs. 2 BDSG vor.[38] § 50 Abs. 2 DSG NRW räumt den Betroffenen ein § 58 Abs. 2 BDSG entsprechendes Löschungsrecht ein (s.o.).

e) Gerichtliche Kontrolle: Anspruch auf Löschung

Personen, deren Daten trotz bestehender Löschpflichten nicht gelöscht worden sind, können ihren Löschungsanspruch auch gerichtlich geltend machen. Eine Klage der betroffenen Personen auf Vernichtung/Löschung der betreffenden Daten vor dem zuständigen ordentlichen Gericht bzw. Verwaltungsgericht hat Aussicht auf Erfolg haben, wenn und

---

[35] So auch nach alter Rechtslage zu § 489 StPO aF.; hierzu *Otto*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl., § 58 Rn. 6; OLG Hamm Beschl. v. 26.2.2021 – 1 VAs 77/20, BeckRS 2021, 6165 Rn. 15; bestätigt durch OLG Hamm Beschl. V. 8.8.2022 – 1 VAs 48/22/, BeckRS 2022, 26713, insb. Rn. 16 ff.

[36] Hierauf weist das OLG Hamm unter Bezugnahme auf das Recht auf informationelle Selbstbestimmung hin und betont die volle gerichtliche Überprüfbarkeit dieses unbestimmten Rechtsbegriffs; OLG Hamm Beschl. V. 8.8.2022 – 1 VAs 48/22/, BeckRS 2022, 26713, Rn. 19.

[37] *Otto*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl., § 58 Rn. 6; OLG Hamm Beschl. v. 26.2.2021 – 1 VAs 77/20, BeckRS 2021, 6165 Rn. 15; bestätigt durch OLG Hamm Beschl. V. 8.8.2022 – 1 VAs 48/22/, BeckRS 2022, 26713, insb. Rn. 16 ff.

[38] Hierauf verweist auch *Otto*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl., § 58 Rn. 10 mwN.

soweit, wie in der Formulierung der Frage unterstellt, eine Löschungspflicht besteht, so dass es auch nicht auf die Überprüfung einer auf die weitere Speicherung gerichteten Ermessensentscheidung der Polizei bzw. der Staatsanwaltschaft ankommt.[39]

f) Datenschutzaufsicht

Datenschutzrechtliche Grundrechtsverletzungen wie auch Verstöße gegen die JI-Richtlinie fallen grundsätzlich in die Kontrollzuständigkeit der/des jeweiligen Datenschutzbeauftragten des Bundes oder des betreffenden Landes. Im Unterschied zur DSGVO sind die Abhilfebefugnisse der Datenschutzbeauftragten nach nationalem Recht in der Regel beschränkt. Hierauf weist auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) in seinem Bericht für das Jahr 2022 hin.[40] Auf der Basis einer Evaluation zur Umsetzung der JI-Richtlinie aus dem Jahr 2022 hat die EU-Kommission Defizite bei der Umsetzung von Art. 47 Abs. 2 JI-Richtlinie auch in Deutschland festgestellt und zum Gegenstand eines im Mai 2022 eröffneten Vertragsverletzungsverfahrens gemacht.[41]

Im Bereich der Aufsicht über die Speicherung personenbezogener Daten im Anwendungsbereich der JI-RL verfügt der BfDI im Unterschied zur nordrhein-westfälischen Datenschutzbeauftragten lediglich über Beanstandungs- bzw. Warnrechte nach § 16 Abs. 2 BDSG, nicht aber über wirksame Abhilfebefugnisse und kann insbesondere die Löschung unzulässig gespeicherter Daten nicht anordnen.[42]

Dies widerspricht den ausdrücklich vorgesehen wirksamen Untersuchungs- und Abhilfebefugnissen nach Art. 47 Abs. 2 JI-RL, die „wirksame Abhilfebefugnisse“ und neben einer Warnung insbesondere auch ein Anweisungsrecht gegenüber Datenverantwortlichen in Bezug auf die Löschung personenbezogener Daten vorsehen.[43]

In der Begründung des an die Bundesrepublik gerichteten Aufforderungsschreibens der EU-Kommission qualifiziert die Kommission diese Rechtslage als Verstoß gegen die Umsetzungspflichten aus der JI-Richtlinie: „Deutschland hat die Bestimmung, wonach die Datenschutzaufsichtsbehörden über wirksame Abhilfebefugnisse unterschiedlicher Art verfügen müssen, nicht ordnungsgemäß umgesetzt. Dazu gehören Warnhinweise, Anordnungen, um Verarbeitungsvorgänge mit den Datenschutzvorschriften in Einklang zu bringen, insbesondere durch die Anordnung von Berichtigungen oder Löschungen personenbezogener Daten oder Einschränkungen der Verarbeitung, sowie eine vorübergehende bzw.

---

[39] S. beispielhaft für ein solches Verfahren OVG NRW v. 14.4.2010, Az. 5 A 479/09 (juris) = DVBl 2010, 852; VG Würzburg v. 29.10.205, Az. W 5 K 14.951 (Juris); korrespondierend für die Löschung durch die StA OLG Frankfurt v. 20.12.2022, Az. 3 VAs 14/22 (juris) = StV-S 2023, 66; ferner die Nachweise in Fn. 35.

[40] S. den 31. Tätigkeitsbericht des BfDI (Fn. 15), BT Drs. 20/6000, S. 48; dies entspricht der Meldung des BfDI an den Europäischen Datenschutzausschuss; vgl. DE_SA_Article_62_LED_questionnaire.pdf (europa.eu). Zu diesem allgemein *Schöndorf-Haubold*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 68 ff.

[41] Aufforderungsschreiben INFR(2022)2023 vom 19.5.2022.

[42] Zur Unionsrechtswidrigkeit *Ziebarth*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 58 Rn. 19; *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 1087 f.

[43] S. bereits oben unter b).

endgültige Beschränkung oder ein Verbot der Verarbeitung. Die Datenschutzaufsichtsbehörden müssen in der Lage sein, ihre Befugnisse gegenüber den Verantwortlichen und/oder den Auftragsverarbeitern auszuüben. Nach Auffassung der Kommission stellt die ordnungsgemäße Umsetzung der Bestimmungen über die Befugnisse der Datenschutzaufsichtsbehörden ein wesentliches Element für die wirksame Gewährleistung des Grundrechts auf den Schutz personenbezogener Daten dar."[44]

§ 60 DSG NRW weist der Landesbeauftragten für Datenschutz und Informationsfreiheit demgegenüber einen Teil der Befugnisse nach der DSGVO zu. Nach § 60 Abs. 3 DSG NRW i.V.m. Art. 58 Abs. 2 d) und f) DSGVO wird die Landesdatenschutzbeauftragte ermächtigt, „den Verantwortlichen […] anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen" bzw. „eine vorübergehende oder endgültige Beschränkung der Verarbeitung einschließlich eines Verbots, zu verhängen". Nach § 500 Abs. 2 Nr. 2 StPO treten die Landesbeauftragten auch in Bezug auf die Aufsicht über die Datenschutzkonformität der Verarbeitung personenbezogener Daten zu repressiven Zwecken an die Stelle des Bundesbeauftragten. Trotz bzw. wegen des auf den dritten Teil des BDSG beschränkten Verweises in § 500 Abs. 1 StPO handeln die Landesbeauftragten im Rahmen ihrer landesrechtlich zugewiesenen Befugnisse.[45]

Ungeachtet der erheblichen Unterschiede in den rechtlich zugewiesenen Befugnissen kommt den Datenschutzbeauftragten eine zentrale Kontrollaufgabe mit Blick auf die Feststellung von Vollzugsdefiziten der vorliegenden Art zu, die von betroffenen Einzelnen regelmäßig nur punktuell und nicht systematisch angegriffen werden können.

- **2. Genügen die Erlasse des Justizministeriums vom 03.08.2022 und vom 18.01.2023, um die Löschung von nicht zu speichernden Daten sicherzustellen, so dass keine Grundrechtsverstöße eintreten?**

Grundsätzlich setzen die Verfassungsmäßigkeit und Grundrechtskonformität der Eingriffe in das Recht auf informationelle Selbstbestimmung bzw. der entsprechenden unions- und konventionsrechtlichen Datenschutzgrundrechte wie auch die richtlinienkonforme Umsetzung der JI-Richtlinie gesetzgeberische Regelungen voraus, die auch die Löschung der Daten innerhalb bestimmter Fristen vorsehen.[46] Die Löschung beendet den Grundrechtseingriff und verhindert eine zweckwidrige Weiterverwendung der Daten. Sie ist damit integraler Bestandteil des verhältnismäßigen Umgangs mit personenbezogenen Daten.

[44] Offizielle Information nach Vertragsverletzungsverfahren im Mai: wichtigste Beschlüsse (europa.eu).
[45] So *Ziebarth*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, 3. Aufl. 2022, Art. 58 Rn. 35. Beispiele aus anderen Bundesländern bei *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 1089. Zu § 60 DSG NRW HK-LDSG NRW/*Heinz-Joachim Pabst*, 1. Aufl. 2020, DSG NRW § 60 Rn. 11 ff.
[46] Hierzu kann auf die Ausführungen zu Frage 1 verwiesen werden.

Auf die in polizeilichen Dateninformationssystemen zu präventiven wie auch zu repressiven Zwecken gespeicherten Daten finden nach §§ 483 Abs. 3, 484 Abs. 4 und 485 S. 4 StPO die Bestimmungen des Polizeigesetzes Anwendung. Nach § 32 I PolG NRW i.V.m. §§ 54, 50 Abs. 3 – 5 DSG NRW sind die Daten insbesondere dann zu löschen, wenn die Datenverarbeitung unzulässig ist, die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich ist oder eine anderweitige rechtliche Verpflichtung zur Löschung besteht. Ergänzend verpflichtet § 32 Abs. 1 S. 4 PolG NRW zur Löschung, wenn der Verdacht einer Straftat gegen die Person entfallen ist.[47]

In Bezug auf die Löschung verfügt die verantwortliche Behörde nicht über ein Ermessen. Die Löschung ist entweder bei Geltendmachung des Anspruchs durch den berechtigten Grundrechtsträger[48] oder jedenfalls im Rahmen der gesetzlich vorgesehenen Überprüfung unter Einhaltung der jeweiligen Prüfpflichten vorzunehmen.

Grundsätzlich enthalten die gesetzlichen Regelungen in Umsetzung der JI-Richtlinie klare Verpflichtungen zur Löschung der nicht weiter zulässig gespeicherten Daten.[49] Weder die Richtlinie noch die gesetzlichen Regelungen können allerdings eine automatische Löschung unzulässig gespeicherter Daten vorschreiben. Einen solchen Automatismus etwa in Gestalt eines Algorithmus gibt es bislang nicht.

Die Erlasse des Justizministeriums vom 3.8.22 und vom 18.1.23 beziehen sich jeweils auf die datenschutzrechtliche Kontrolle von Verfahrensrückmeldungen nach § 482 StPO im Wege der Mitteilung nach Nr. 11 Abs. 2 MiStra durch die Landesbeauftragte für Datenschutz und Informationsfreiheit, bei der sich erhebliche Unzulänglichkeiten gezeigt hatten.

Fehler betrafen das Fehlen einer Rückmeldung nach Nr. 11 Abs. 2 MiStra, die fehlerhafte Verwendung der erforderlichen Kennziffer über die Art des Verfahrensausgangs, das Fehlen einer Einzelfallprüfung der Erforderlichkeit der weiteren Speicherung durch die Polizeibehörden sowie das Fehlen ausreichender Informationen zur Entscheidung über die weitere Speicherung. Es handelt sich damit um Fehler an der Schnittstelle einer Datenspeicherung zwischen Staatsanwaltschaft und Polizei, die im Ergebnis insbesondere dazu führen, dass Daten auch bei Nichtvorliegen eines Restverdachts weitergespeichert werden bzw. nicht gelöscht werden, da das Fortbestehen der Erforderlichkeit entweder nicht geprüft oder fälschlich unterstellt wird.

In Bezug auf unterbliebene und fehlerhafte Mitteilungen seitens der Staatsanwaltschaft sind die nicht außenwirksamen Erlasse grundsätzlich geeignet, auf die ordnungsmäßige Anwendung der gesetzlichen Vorschriften hinzuwirken und damit auch die von der Daten-

[47] S. bereits oben zu Frage 1 c). Ausnahmen von der Löschung sind in § 32 III PolG NRW und § 50 III DSG NRW vorgesehen. Ihre Richtlinienkonformität ist zum Teil strittig.
[48] S. oben bei Frage 1 d).
[49] S. oben bei Frage 1.

schutzbeauftragten beanstandeten Vollzugs-Defizite zu beseitigen. Die Erlasse adressieren allerdings lediglich die Staatsanwaltschaften und binden die für die Löschung letztverantwortlichen Polizeibehörden nicht, wenn die Daten in polizeilichen Informationssystemen gespeichert sind. Handelt es sich daher um Daten, die in polizeilichen Informationssystem gespeichert werden, tragen die Erlasse lediglich zur Verbesserung des Vollzugs seitens der StA bei und leisten insoweit auch einen Beitrag zur Reduktion des Vollzugsdefizits.

Sofern die Datenschutzbeauftragte auf bestehende Vollzugsprobleme seitens der Polizeibehörden hinweist, könnte/müsste diesen durch entsprechende Verwaltungsvorschriften des zuständigen Innenministeriums bzw. der Polizeibehörden entgegengewirkt werden.[50] Erforderlich wäre eine den Erlassen korrespondierende Verpflichtung der Polizei zur Prüfung und Löschung in den Fällen einer entsprechenden Mitteilung durch die StA.

Insgesamt scheint es sich um ein bereits seit längerem bekanntes Problem zu handeln, das in der Literatur beschrieben und seitens verschiedener Datenschutzbeauftragter wiederholt gerügt worden ist.[51]

Nach Art. 5 JI-RL müssen die Mitgliedstaaten vorsehen, dass für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen sind. Weiter ist durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden. Auch die Verantwortlichen müssen auf der Grundlage mitgliedstaatlicher Umsetzungsvorschriften nach Art. 19 und 20 JI-RL „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen“ umsetzen, „um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung“ mit der JI-RL erfolgt. Diese Maßnahmen sind erforderlichenfalls zu überprüfen und zu aktualisieren. Darüber hinaus müssen die Verantwortlichen nach Art. 20 JI-RL „angemessene technische und organisatorische Maßnahmen“ ergreifen, um bei der Verarbeitung den Datenschutzgrundsätzen und Garantien gerecht zu werden.

Um die Löschung sicherzustellen bedarf es deshalb effektiver praktischer Sicherungsmechanismen, vorrangig in Gestalt von allgemeinen Lösch- wie auch Löschprüffristen,[52] aber

[50] Nr. 32 der Verwaltungsvorschrift zum PolG NRW (VVPolG NRW), Runderlass d. Innenministeriums v. 19.12.2003 – 44.1-2001 bestimmt zwar, dass Ermittlungen in angemessenem Umfang von Amts wegen durchzuführen sind, wenn der Verdacht einer unrichtigen Datenspeicherung besteht. Die betreffenden Daten sind während der Prüfung mit einem Sperrvermerk zu versehen. Die Norm sieht aber nicht vor, dass auch die Polizeibehörden in kürzeren Abständen die datenschutzrechtliche Konformität der gespeicherten Daten systematisch überprüfen müssten. Ob es darüber hinaus Verwaltungsvorschriften seitens der Polizeibehörden in NRW gibt, entzieht sich meiner Kenntnis.

[51] S. nur *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 844 mwN. und Abhilfevorschlägen; ferner BeckOK PolR NRW/*Arzt*, 25. Ed. 15.4.2023, PolG NRW § 22 Rn. 57 ff.

[52] *Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 301.

darüber hinausgehend in zusätzlichen flankierenden Regelungen, zumal die Lösch- und Löschprüffristen zum Teil sehr lang bemessen sind und zudem nicht auf fehlerhafte Datenspeicherungen, sondern auf die rechtmäßige Speicherung zulässig erhobener und verwerteter Daten abstellen.

Ergänzende Bestimmungen finden sich im Datenschutzrecht: So sieht § 54 Abs. 4 DSG NRW ähnlich wie § 75 Abs. 4 BDSG vor, dass die für die Datenverarbeitung verantwortliche Stelle, d.h. die speichernde Polizeibehörde „unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschungsfristen" „für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen" hat, „dass diese Fristen eingehalten werden".

Neben der fehlerfreien Übermittlung der korrekten Kennziffern kommt es hinsichtlich der den Fragen zugrunde liegenden Problematik zum einen vor allem auf die Gewährleistung einer ausreichenden Informationsgrundlage sowie auf regelmäßige Prüf- und Erkundigungspflichten seitens der speichernden Polizeibehörden an.[53]

Mögliche weitere Maßnahmen zur Behebung der Vollzugsprobleme wären etwa:

- den Erlassen entsprechende Verwaltungsvorschriften des Innenministeriums / seitens der Polizei etwa zur Pflicht der regelmäßigen Anforderung von Informationen nach § 472 Abs. 2 StPO,[54]
- die gesetzliche, untergesetzliche oder verwaltungsinterne Normierung weiterer, klar bestimmter und insb. auch kürzerer Prüffristen jenseits bzw. in Ausfüllung von § 54 Abs. 4 DSG NRW und § 75 Abs. 4 BDSG[55],
- die Einführung automatisierter Prüfroutinen und –verfahren,[56]

[53] *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 845: automatisierte regelmäßige Erkundigung der Polizeibehörden bei den Staatsanwaltschaften, um Wissensdefizite über Verfahrensausgänge und hierauf basierende unzulässige Weiterspeicherung von Daten zu vermeiden. BeckOK PolR NRW/*Arzt*, 25. Ed. 15.4.2023, PolG NRW § 22 Rn. 59 f. verweist auf einen möglichen Konflikt mit der auch im Rahmen der EMRK geschützten Unschuldsvermutung.

[54] Vgl. etwa den Verweis des VG Köln Urt. v. 20.5.2021 – 20 K 418/18, BeckRS 2021, 23660 Rn. 26 und 40 auf die Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS) (RdErl. d. Innenministeriums NRW v. 25.08.2000, IV A 5 - 6420/1, MBl. NRW. 2000 S. 1370); zum Problem der unzureichenden Informationsgrundlage auch BeckOK PolR NRW/*Arzt*, 25. Ed. 15.4.2023, PolG NRW § 22 Rn. 62 mwN.

[55] § 54 Abs. 4 DSG NRW verpflichtet die Datenverantwortlichen unbeschadet anderweitiger Höchstspeicherfristen oder Löschungsfristen dazu, „für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden."; Beispiele für Vorschriften mit Prüffristen und Prüfungsterminen finden sich bei *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 853 f.

[56] *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 856 ff. mit dem Hinweis, dass Löschprüffristen „keine Regelspeicherfristen" sind, sowie dem Vorschlag automatisierter Löschroutinen und Prüf-Wiedervorlagen.

- die zu kontrollierende Verpflichtung zu regelmäßigen Prüfungen vor Ablauf der Prüf- und Speicherhöchstfristen, um systematisch sicherzustellen, dass die gebotenen Datenprüfungen, sowie Datenlöschungen auch durchgeführt werden.

Etwaige Löschungsdefizite stellen nicht notwendig ein Problem auf der Ebene der Gesetzgebung, sondern ein Vollzugsproblem dar. Da die gesetzlichen Regelungen die Löschungspflicht sowie einen korrespondierenden subjektiv-rechtlichen Löschungsanspruch klar vorsehen, besteht gesetzgeberischer Handlungsbedarf dann, wenn die Vollzugsdefizite mit Hilfe der Erlasse und unter Verweis auf die Verantwortlichkeit der Datenverantwortlichen nicht behoben werden können.

Anhaltspunkte für eine Verantwortungsteilung zwischen Gesetzgeber und Verwaltung finden sich in der jüngsten Entscheidung des Bundesverfassungsgerichts zur automatisierten Datenverarbeitung: Das Gericht erachtet eine Aufteilung der Regelungen zwischen Gesetzgeber und Verwaltung für zulässig, solange der Gesetzesvorbehalt zu Gunsten der wesentlichen Grundlagen (hier zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethode) gewahrt wird, der Gesetzgeber die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten in abstrakt-genereller Form, verlässlich dokumentiert und publiziert ermächtigt und die verfassungsrechtlich gebotene Kontrolle etwa durch Datenschutzbeauftragte wahrgenommen wird.[57]

Sofern es sich allerdings um ein – ggf. bewusst in Kauf genommenes – Dauerproblem handelt, ist aber nicht auszuschließen, dass sich Vollzugsdefizite auf die Beurteilung der Verhältnismäßigkeit und damit der Verfassungsmäßigkeit polizeilicher Datenspeicherungen insgesamt auswirken könnten. In diese Richtung weist auch die Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023: Je fehleranfälliger sich ein System zur Datenspeicherung erweist, desto stärker verschiebt sich die Abwägungsentscheidung zu Gunsten des Grundrechtsschutzes.[58] Fehlerintensive Regelungen werden als eingriffsintensiver qualifiziert.

- **3. In der Entscheidung des BVerfG vom 16.2.2023 wurde auf die Problematik hingewiesen. Darin heißt es: „Denn es können sich softwaregestützt neue Möglichkeiten einer Vervollständigung des Bildes von einer Person ergeben, wenn Daten und algorithmisch errechnete Annahmen über Beziehungen und Zusammenhänge aus dem Umfeld der Betroffenen einbezogen werden. Der Grundsatz der Zweckbindung könnte dem Eingriffsgewicht dann für sich genommen nicht hinreichend Rechnung tragen. Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer**

[57] BVerfG v. 16.2.2023, NJW 2023, 1196 (Leitsätze – automatisierte Datenanalyse).
[58] In diese Richtung auch BVerfG NJW 2023, 1196 (1204 Rn. 90 – automatisierte Datenanalyse).

die softwaregestützten Verknüpfungen nachvollzogen werden können.“ Wo liegen nach Ansicht der Sachverständigen die verfassungsrechtlichen Probleme in Bezug auf die Nichtlöschung von Daten, was die Landesdatenschutzbeauftragte in ihrem Bericht auf den Seiten 52 – 55 kritisiert?

Über die verfassungswidrige Nichtlöschung (als Grundrechtsproblem an sich) hinaus besteht für die somit nicht länger rechtmäßig gespeicherten Daten das Risiko einer zweckwidrigen weiteren Verwendung. Automatisierte Datenverarbeitungsvorgänge erhöhen die Gefahr eines Zugriffs auf nicht gelöschte Daten, die ggf. unbemerkt Gegenstand einer übergreifenden Datenanalyse oder Datenauswertung werden können.

In der Entscheidung vom 16.2.2023 hat das Bundesverfassungsgericht die Voraussetzungen für eine verfassungskonforme Ausgestaltung entsprechender gesetzlicher Ermächtigungen formuliert. Diese Voraussetzungen sind bereits in Bezug auf rechtmäßig gespeicherte Daten aufgrund der speziellen Belastungseffekte und der variierenden Belastungsintensität komplex. Schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung sind nur unter engen Voraussetzungen zulässig. Eine Reihe von Daten, die im Wege besonders intensiver Grundrechtseingriffe gewonnen wurden, sollen aus den automatisierten Datenverarbeitungsvorgängen aufgrund ihres hohen Eingriffsgewichts ausgenommen werden.

Keinesfalls dürfen löschungspflichtige und damit nicht länger gerechtfertigt gespeicherte Daten in eine automatisierte Auswertung einbezogen werden.[59] Eine ansonsten zulässige und gesetzlich geregelte Datenanalyse, die unter diesen Voraussetzungen einen verhältnismäßigen und damit gerechtfertigten Grundrechtseingriff darstellt, führt dann zu verfassungsrechtlich unzulässigen neuen Eingriffen in das Recht auf informationelle Selbstbestimmung, wenn sie sich auf Daten bezieht, deren Speicherung nicht länger zulässig ist.

- **4. In der Entscheidung des BVerfG heißt es weiter: „Dem Wortlaut nach lassen sie (Anm.: die Regelungen in den beiden Polizeigesetzen) zudem sehr weitreichende Methoden der automatisierten Datenanalyse und -auswertung zu. Der Gesetzgeber hat nicht eingegrenzt, welche Methoden der Analyse und Auswertung erlaubt sind. Die angegriffenen Vorschriften ermöglichen auch ein „Data-Mining“ bis hin zur Verwendung selbstlernender Systeme (KI). Dabei sind insbesondere auch offene Suchvorgänge zulässig. Die Datenauswertung oder -analyse darf darauf zielen, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, aus denen dann, möglicherweise auch mit Hilfe weiterer automatisierter Anwendungen, weitere Schlüsse gezogen werden.**

[59] *Müller/Schwabenbauer*, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 852; BeckOK PolR NRW/*Arzt*, 25. Ed. 15.4.2023, PolG NRW § 22 Rn. 16.

Die Vorschriften schließen auch bezüglich der erzielbaren Suchergebnisse nichts aus. Nach dem Wortlaut könnte das Suchergebnis in maschinellen Sachverhaltsbewertungen bestehen – bis hin zu Gefährlichkeitsaussagen über Personen im Sinne eines „predictive policing". Es könnten also mittels Datenanalyse oder -auswertung neue persönlichkeitsrelevante Informationen erzeugt werden, auf die ansonsten kein Zugriff bestünde. Diese potenzielle Weite erzielbaren neuen Wissens wird auch nicht durch eingriffsmildernde Regelungen zu dessen Verwendung flankiert."
Wo liegen nach Ansicht der Sachverständigen die verfassungsrechtlichen Probleme in Bezug auf die Nichtlöschung von Daten, was die Landesdatenschutzbeauftragte in ihrem Bericht auf den Seiten 52 – 55 kritisiert?

Je intensiver die mittels der automatisierten Datenverarbeitung vorgenommenen Grundrechtseingriffe wirken,[60] desto größer wird auch das Eingriffsgewicht in Bezug auf ohnehin unzulässig einbezogene Daten. Insoweit ist auf die Beantwortung der Frage 3 zu verweisen.

- **5. Wie ist am ehesten verfassungsrechtlich sicherzustellen, dass die Staatsanwaltschaften die Vorgaben der Landesdatenschutzbeauftragten beachten und erforderliche Daten gelöscht werden?**

Im Rahmen der Rechtsbindung der Staatsanwaltschaften genügt das gesetzgeberische, hinreichend bestimmte Löschungsgebot grundsätzlich den verfassungsrechtlichen Anforderungen. Von einer Befolgung muss zunächst ausgegangen werden.

Soweit im Bericht der Datenschutzbeauftragten Vollzugsdefizite festgestellt werden, kann diesen auf der Vollzugsebene mit den Mitteln des verwaltungsinternen Organisationsrechts begegnet werden. Insoweit ist zu erwarten, dass die Erlasse des Justizministeriums ebenso wie der Bericht der Datenschutzbeauftragten zu einer Behebung der Vollzugsprobleme führen.[61]

Sollte sich bei weiteren Überprüfungen herausstellen, dass diese Maßnahmen nicht ausreichen, müsste der Gesetzgeber insbesondere auch aus unionsrechtlichen Gründen in Erwägung ziehen, auch für die Staatsanwaltschaften Prüfroutinen gesetzlich zu verankern und/oder den Datenschutzbeauftragten gesetzlich effektivere Abhilfebefugnisse und Anordnungsrechte einzuräumen.

[60] Allgemein zum Einsatz von KI durch Sicherheitsbehörden *Hornung*, Künstliche Intelligenz zur Auswertung von Social Media Massendaten. Möglichkeiten und rechtliche Grenzen des Einsatzes KI-basierter Anaylsetools durch Sicherheitsbehörden, AöR 147 (2022), 1 ff.; *Rademacher*, Predictive Policing im deutschen Polizeirecht, AöR 142 (2017), S. 366 ff.
[61] Zu wiederkehrenden Beanstandungen s. aber auch oben bei Fn. 51.

- **6. Benötigen wir ein spezielles Datenverarbeitungsgesetz in NRW, aus dem sich für den Bürger auch die Rechte auf Löschung ergeben, in dem eine gesetzliche Definition des Begriffs „Restverdacht“ verankert ist, in dem Löschfristen gesetzlich verankert sind?**

Zwar ist zuzugeben, dass sich das Rechtsregime nicht gerade übersichtlich aus einer Reihe unterschiedlicher gesetzlicher Bestimmungen ergibt. Dies ist allerdings vorrangig auf die unterschiedliche verfassungsrechtliche Zuständigkeit für die Gesetzgebung im Bundesstaat zurückzuführen. Soweit sich die Frage lediglich auf die Rechtslage in NRW bezieht, genügt auch ein auf PolG und DSG verteiltes Regelungsregime grundsätzlich den Anforderungen der JI-Richtlinie wie auch rechtsstaatlichen Bestimmtheits- und Transparenzanforderungen.

Hiervon zu unterscheiden ist die Frage nach möglichen Regelungsinhalten. Das Recht auf Löschung ist, wie oben in Frage 1 dargelegt, bereits gesetzlich verankert. Löschfristen sind (nur) teilweise auch gesetzlich bestimmt und insbesondere bei Datenerhebungen vorgesehen, die mit schwerwiegenden Grundrechtseingriffen verbunden sind. Gesetzlich fixierte Löschfristen sind aus Gründen der Rechtssicherheit und des Grundrechtsschutzes grundsätzlich vorzugswürdig. Da Prüffristen nicht zugleich auch Höchstspeicherfristen darstellen, können sie Regelungen zur Festlegung von Speicherfristen auch nicht ersetzen.[62]

Weder Höchstspeicherfristen noch Prüffristen vermögen eine Ausschöpfung der Speicher- und Prüffristen aus sich heraus zu rechtfertigen. Eine nach der JI-RL und den jeweiligen Bestimmungen des Bundes- und Landesrechts erforderliche Prüfung der Erforderlichkeit der Speicherung wird durch sie nicht entbehrlich.[63]

Bei dem Begriff des Restverdachts handelt es sich um einen unbestimmten Rechtsbegriff, den die Rechtsprechung im Zusammenhang mit § 484 Abs. 2 StPO heranzieht und den § 22 Abs. 3 PolG NRW entsprechend für die Speicherung in polizeilichen Datensystemen aufgreift. Nur in diesem Kontext des Polizeirechts verfügt der nordrhein-westfälische Gesetzgeber über die Zuständigkeit zur Konkretisierung dieses Begriffs.

Eine Legaldefinition erhöht die Rechtssicherheit und führt zu größerer Rechtsklarheit, scheint mir aber nicht aus verfassungsrechtlicher Sicht geboten. Vielmehr ist es grundsätzlich ausreichend, wenn die Gerichte die Auslegung des Begriffs durch Polizei und Staatsanwaltschaft voll überprüfen.[64]

---

[62] S. hierzu BeckOK PolR NRW/*Arzt*, 25. Ed. 15.4.2023, PolG NRW § 22 Rn. 39 f. zu fehlenden Höchstspeicherfristen insb. in § 22 PolG NRW.

[63] S. hierzu bereits oben bei Fn. 36; ferner BeckOK PolR NRW/*Arzt*, 25. Ed. 15.4.2023, PolG NRW § 22 Rn. 42 ff., Rn. 50 zur Unverhältnismäßigkeit der Regelung in § 22 Abs. 2 S. 5 PolG NRW.

[64] Ähnlich für den Begriff der Erforderlichkeit OLG Hamm Beschl. V. 8.8.2022 – 1 VAs 48/22/, BeckRS 2022, 26713, insb. Rn. 19.