LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

LEHRSTUHL FÜR DEUTSCHES, EUROPÄISCHES UND INTERNATIONALES STRAFRECHT, STRAFPROZESSRECHT, WIRTSCHAFTSSTRAFRECHT UND DAS RECHT DER DIGITALISIERUNG

PROF. DR. MARK A. ZÖLLER

LMU · Geschwister-Scholl-Platz 1 · 80539 München

Herr
Präsident des Landtags Nordrhein-Westfalen
André Kuper, MdL
Platz des Landtags 1
40221 Düsseldorf

per E-Mail: anhoerung@landtag.nrw.de

Dr. Tanja Niedernhuber

Telefon +49 (0)89 2180-5726
Telefax +49 (0)89 2180-5675

tanja.niedernhuber@jura.uni-muenchen.de

Postanschrift
Prof.-Huber-Platz 2
80539 München

Büroanschrift
Ludwigstr. 29/IV
80539 München

München, 23.05.2023

Schriftliche Stellungnahme

zum Thema „Löschung von Daten als Ergebnis staatsanwaltschaftlicher Ermittlungen unter Betrachtung des Urteils des Bundesverfassungsgerichts – Vorlage 18/1027"

im Rahmen der Anhörung des Rechtsausschusses am 5. Juni 2023

Sehr geehrter Herr Präsident, sehr geehrter Herr Vorsitzender des Rechtsausschusses, sehr geehrte Damen und Herren Abgeordnete,

für die Einladung zur oben genannten Anhörung und die Gelegenheit zur Stellungnahme möchte ich mich herzlich bedanken. Zu Ihrem Fragenkatalog nehme ich wie folgt Stellung:

Frage 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?

Die Speicherung von personenbezogenen Daten stellt einen Eingriff in das verfassungsrechtlich geschützte Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung dar.[1] Ein solcher Eingriff bedarf der Rechtfertigung durch ein normklares und verhältnismäßiges parlamentarisches Gesetz. Die §§ 483 ff. StPO und entsprechende polizeirechtliche Vorschriften normieren eine solche Rechtfertigung. Diese gilt allerdings nur so lange, wie die vom Gesetz vorgesehenen Voraussetzungen vorliegen. Sobald personenbezogene Daten gelöscht werden müssen, aber nicht ge-

[1] BVerfGE 65, 1, 43 f.; BVerfG NVwZ 1988, 1119.

löscht, sondern weiterhin gespeichert werden, stellt dies einen nicht gerechtfertigten Grundrechtseingriff dar.[2] Einen solchen gilt es tunlichst zu vermeiden. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 16. Februar 2023 ausführlich geschildert, wie tief die mit einer Datenverarbeitung verbundenen Grundrechtseingriffe insbesondere bei automatisierter Datenanalyse, wie sie auch in Nordrhein-Westfalen zum Einsatz kommt, sein können. Eine großflächige, unzulässige Speicherung personenbezogener Daten durch staatliche Stellen kann das Vertrauen der Bevölkerung in die Arbeit von Staatsanwaltschaften und Polizeibehörden stark erschüttern.

Frage 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?

Nein, die Erlasse des Justizministeriums genügen nicht, um die Löschung von nicht zu speichernden Daten sicherzustellen und Grundrechtsverstöße zu verhindern. Sie enthalten einen bloßen Appell an die datenverarbeitenden Stellen, auf den Datenschutz zu achten.

Die Generalstaatsanwältin und Generalstaatsanwälte in Düsseldorf, Hamm und Köln haben ausweislich ihrer Berichte vom 13./14. März 2023[3] den Staatsanwaltschaften ihres Geschäftsbereichs die Erlasse „mit der Bitte um Kenntnisnahme und Beachtung" übersandt. Die Erlasse müssen im Anschluss daran aber erst noch von jedem einzelnen Behördenmitarbeiter zur Kenntnis genommen und jeden Tag aufs Neue beachtet werden. Eine Garantie, dass das auch so geschieht, ist mit der bloßen Übersendung der Erlasse nicht verbunden. Solange Menschen etwa darüber entscheiden, ob der Polizei nach § 482 Abs. 2 StPO eine Mitteilung gemacht (StA) bzw. ob eine solche Mitteilung zur Bereinigung des Datenbestands herangezogen wird (Polizei), kann man Fehler und Nachlässigkeiten nicht zuverlässig verhindern. Sie lassen sich nur mühsam im Nachhinein durch datenschutzrechtliche Aufsicht und Kontrolle entdecken und korrigieren. In diesem Zeitpunkt ist aber das sprichwörtliche Kind bereits in den Brunnen gefallen, das heißt der jeweilige, nicht gerechtfertigte Grundrechtseingriff ist eingetreten.

---

[2] *Worms*, in: BeckOK Datenschutzrecht, 43. Ed., 1.11.2021, § 58 BDSG Rn. 40 f.

[3] Wiedergegeben im Schriftlichen Bericht über die Sitzung des Rechtsausschusses des Landtags Nordrhein-Westfalen am 22.03.2023 zu TOP „Löschung von Daten als Ergebnis staatsanwaltlicher Ermittlungen unter Betrachtung des Urteils des Bundesverfassungsgerichts" (MMV 18/1027), S. 4.

Es bedarf daher vielmehr einer technischen Lösung (siehe unten Frage 5). *Roßnagel* hat das vor knapp 20 Jahren auf den Punkt gebracht: „*Ohne technische Unterstützung droht Recht in einer technikgeprägten Welt folgenlos zu bleiben. Recht ist auf rechtsgemäße Technik angewiesen. Informationelle Selbstbestimmung ist durch, nicht gegen Technik zu ermöglichen. Schutz durch Technik ist oft die einzig mögliche Antwort auf Probleme der Globalisierung der Datenflüsse, der dynamischen Technikentwicklung und der zunehmenden Intransparenz der Systeme*."[4]
Die elektronische Führung von Verfahrensakten und Datei- bzw. Informationssystemen bietet daher die Chance, durch die automatisierte Versendung von Mitteilungen und durch automatisierte Löschung jeweils bei Vorliegen der gesetzlichen Voraussetzungen Grundrechtseingriffe zu verhindern.
Was die Erlasse nur leisten können, ist eine Entscheidungshilfe für die Vergabe von Erledigungskennziffern. Dort, wo (noch) menschliche Entscheidungen zwischen verschiedenen Erledigungskennziffern erforderlich sind, haben die Erlasse einen Sinn. Ein Erlass könnte darüber hinaus die Staatsanwaltschaften und Polizeibehörden zu einer besseren Kooperation mit der Landesdatenschutzbeauftragten auffordern, damit die verfassungsrechtlich gebotene Datenschutzkontrolle erfolgen kann, ohne dass der Klageweg beschritten werden muss.[5]

Frage 3: (...) 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?
Jede unterlassene Löschung zu löschender personenbezogener Daten stellt einen Grundrechtseingriff dar. Die zitierte Passage des Urteils des Bundesverfassungsgerichts betrifft die erhöhte Eingriffsintensität von Datenspeicherungen in Datei- bzw. Informationssystemen mit automatisierter Datenanalyse oder Datenauswertung.
Je mehr Daten über eine Person in behördlichen Datei- bzw. Informationssystemen gespeichert sind, desto vollständiger ist das Bild, das staatliche Stellen von der konkreten Person gewinnen. Im Wege der automatisierten Datenanalyse bzw. Datenauswertung mehrerer personenbezogener Daten lassen sich recht einfach Bewegungs-, Verhaltens- oder Beziehungsprofile oder noch umfassendere Persönlichkeitsbilder erstellen. Dadurch wird das Gewicht des individuellen

[4] *Roßnagel*, Informatik Spektrum 2005, 462, 469.
[5] Vgl. LDI NRW, 27. Bericht 2022, S. 54.

Grundrechtseingriffs deutlich erhöht.[6] Mit einem derart erhöhten Grundrechtseingriff müssen zwingend höhere Eingriffsschwellen verbunden sein.[7] Das gilt nicht nur für die Erhebung, sondern auch für die weitere Speicherung von Daten. Die Befugnisse zur weiteren Speicherung von personenbezogenen Daten, die nach einem erledigten Strafverfahren für dieses nicht mehr benötigt werden, sind daher sehr restriktiv zu handhaben. Werden zu löschende Daten nicht gelöscht und ist der Datenbestand daher größer als er sein dürfte, wirkt sich das auch auf die Eingriffsintensität zukünftig zu erhebender Daten aus, die den vorhandenen Datenpool weiter vergrößern.

Eine unzulässige weitere Speicherung personenbezogener Daten nach einem Freispruch oder einer Verfahrenseinstellung stellt einen noch wesentlich intensiveren Grundrechtseingriff dar, wenn die Person bei einer Suche in den behördlichen Datenbanken auftaucht und mit einem Delikt in Verbindung gebracht wird, das sie nach behördlicher oder gerichtlicher Feststellung nicht begangen hat.

Frage 4: (…) 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?

Das Bundesverfassungsgericht arbeitet in der zitierten Passage heraus, dass das Eingriffsgewicht auch durch die Methoden der Datenverarbeitung erhöht werden kann. So können Methoden automatisierter Datenanalyse oder Datenauswertung neue personenbezogene Informationen und Zusammenhänge zu Tage fördern, die durch manuelle Datenverarbeitung nicht oder nur mit unverhältnismäßigem Aufwand erkennbar wären. Die hessischen und hamburgischen Regelungen erlauben es der Polizei, „*mit einem Klick umfassende Profile von Personen, Gruppen und Milieus zu erstellen und auch zahlreiche rechtlich unbeteiligte Personen weiteren polizeilichen Maßnahmen zu unterziehen, die in irgendeinem Zusammenhang Daten hinterlassen haben, deren automatisierte Auswertung die Polizei auf die falsche Spur zu ihnen gebracht hat*“[8].

[6] BVerfG NJW 2023, 1196, 1201 f.
[7] BVerfG NJW 2023, 1196, 1199 ff.
[8] BVerfG NJW 2023, 1196, 1212.

Verfassungsrechtlich problematisch an diesen Regelungen ist das Fehlen einer Eingrenzung der Datenverarbeitungsmethoden oder sonstiger Schranken, welche die Eingriffstiefe begrenzen würden. Für derartig tiefe Grundrechtseingriffe ist im Bereich des Gefahrenabwehrrechts mindestens eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut erforderlich.[9] Eine solche liegt bei der weiteren Speicherung personenbezogener Daten nach Erledigung eines Strafverfahrens jedoch meistens nicht vor. Die hessischen und hamburgischen Regelungen sind aus diesem Grund verfassungswidrig, weil sie die Weiterverarbeitung personenbezogener Daten mittels automatisierter Datenanalyse zur „vorbeugenden Bekämpfung" bestimmter Straftaten gestatten. Der Verarbeitungszweck der Strafverfolgungsvorsorge ist dabei von vornherein ausgeschlossen und für die Verhütung von (zu erwartenden) Straftaten genügen die vorgesehenen Eingriffsschwellen nicht den Vorgaben des Bundesverfassungsgerichts (konkretisierte Gefahr für ein bedeutendes Rechtsgut).[10]

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

Durch eine technische Lösung ist am ehesten sicherzustellen, dass die Staatsanwaltschaften nicht mehr erforderliche Daten zeitnah löschen. Gesetze, Erlasse und Schulungen können zwar Staatsanwältinnen und Staatsanwälte immer wieder daran erinnern, dass Daten zu löschen sind und Verfahrenserledigungen den Polizeibehörden mitgeteilt werden müssen. Das kann jedoch nicht zuverlässig verhindern, dass im Einzelfall die Löschung oder Mitteilung unterbleibt. Dieser Gedanke liegt auch § 71 BDSG zugrunde.

Den ohnehin überlasteten Staatsanwaltschaften wäre mit einer technischen Lösung besser gedient, welche die gesetzlichen Löschungs- und Aussonderungsprüffristen – jeweils gekoppelt an die Art der Verfahrenserledigung – bereits eingespeichert hat und automatisch die Mitteilung an die Polizeibehörden sendet, Daten löscht oder an die Prüfung der Datenlöschung erinnert.[11] Denkbar wäre eine automatische Datenlöschung, die erforderlichenfalls aktiv verhindert werden muss, wenn die Daten weiterhin gespeichert werden sollen. Da die weitere Datenspeicherung

[9] BVerfG NJW 2023, 1196, 1212.
[10] BVerfG NJW 2023, 1196, 1212 ff.
[11] Vgl. auch § 71 Abs. 2 S. 2 BDSG; *Borell/Schindler*, DuD 2019, 767, 770.

die Ausnahme und die Löschung die Regel sein soll, könnte der Datenschutz auf diesem Wege besser gewährleistet werden. Eine solche aktive weitere Speicherung der Daten könnte eine Push-Nachricht an den behördeninternen Datenschutzbeauftragten senden, der/die die konkrete weitere Speicherung daraufhin überprüfen könnte. Das würde eine unkontrollierte weitere unzulässige Datenspeicherung zuverlässiger verhindern als mahnende Worte der jeweiligen Vorgesetzten. Eine solche technische Lösung hätte auch den Vorteil, dass sich nicht jeder einzelne Staatsanwalt mit den Löschungsregelungen auskennen muss und seine Kapazitäten auf das Kerngeschäft fokussieren kann.

Sobald also ein Staatsanwalt eine bestimmte Erledigungskennziffer in das Datenverarbeitungsprogramm einträgt, könnte dieses sämtliche weiteren gesetzlich vorgesehenen, datenschutzrechtlich erforderlichen Schritte ausführen. Damit könnte ggf. auch sichergestellt werden, dass erforderliche Löschungen nicht nur punktuell – wie von der Datenschutzbeauftragten bemängelt[12] –, sondern an allen relevanten Stellen vorgenommen werden.

Frage 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?

Das Recht auf Löschung personenbezogener Daten benötigt grundsätzlich keine zusätzliche gesetzliche Verankerung. Es folgt bereits unmittelbar aus dem Grundgesetz. Die Speicherung ist umgekehrt der rechtfertigungsbedürftige Akt. Sobald sie nicht mehr zulässig ist, sind die Daten von Amts wegen und nicht erst auf Antrag der betroffenen Personen zu löschen.

Dass dessen ungeachtet eine gesetzliche Regelung des Löschungsanspruchs eine nützliche Hilfestellung für die Praxis sein kann, soll hier nicht in Abrede gestellt werden. Das Bundesdatenschutzgesetz, das über § 500 StPO für die Datenverarbeitung durch Staatsanwaltschaften und Polizeibehörden Anwendung findet, enthält daher in § 75 Abs. 2 BDSG die Pflicht des datenschutzrechtlich Verantwortlichen, personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist. Damit korrespondiert ein Anspruch der betroffenen Person auf unverzügliche Löschung der sie betreffenden Daten in den genannten Fällen nach § 58 Abs. 2 BDSG. Beide Regelungen sind lediglich

[12] LDI NRW, 27. Bericht 2022, S. 54.

deklaratorisch.[13] Sie werden ergänzt bzw. verdrängt durch die vorrangigen bereichsspezifischen Vorschriften in § 489 Abs. 1 und § 494 Abs. 1 StPO,[14] welche weitergehende Löschungspflichten normieren.

Das Oberlandesgericht Hamm hat in jüngerer Vergangenheit die Löschungsregelungen, insbesondere die im Einzelfall vorzunehmende Prüfung der Erforderlichkeit einer weiteren Datenspeicherung nach § 484 bzw. § 485 StPO unter Berücksichtigung der Voraussetzungen eines Restverdachts, genauer konturiert.[15]

Eine gesetzliche Regelung in Nordrhein-Westfalen wie in der Fragestellung beschrieben ist somit nicht erforderlich. Das Land Nordrhein-Westfalen besitzt darüber hinaus auch gar nicht die Gesetzgebungskompetenz zum Erlass eines solchen Gesetzes. Die Speicherung von Daten aus einem Strafverfahren zum Zweck der Strafverfolgungsvorsorge nach § 484 StPO bzw. zur Vorgangsverwaltung nach § 485 StPO fällt unter die konkurrierende Gesetzgebungskompetenz nach Art. 74 Abs. 1 Nr. 1 Alt. 4 GG (gerichtliches Verfahren).[16] Der Bund hat von seiner Gesetzgebungskompetenz hinsichtlich der Löschungsfristen mit den Regelungen in § 484 und § 489 StPO abschließend Gebrauch gemacht, sodass für eine Landesregelung kein Raum verbleibt. Eine landesrechtliche Regelung kann eine weitere Datenspeicherung lediglich zu präventiven Zwecken vorsehen.[17]

Es besteht lediglich die Möglichkeit, in einer Errichtungsanordnung kürzere Löschungsfristen festzulegen, § 489 Abs. 4 i.V.m. § 490 StPO. Diese Möglichkeit haben jedoch nur die jeweils für das Datei- oder Informationssystem Verantwortlichen, nicht der Landtag Nordrhein-Westfalen.

---

[13] *Benamor*, K&R 2023, 95, 96.
[14] Siehe § 500 Abs. 2 Nr. 1 StPO.
[15] OLG Hamm, Beschl. v. 26.2.2021 – III-1 VAs 74/20, 1 VAs 74/20; Beschl. v. 26.2.2021 – 1 VAs 77/20; Beschl. v. 8.8.2022 – 1 VAs 48/22.
[16] *Müller/Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G, Rn. 572, 577; *Uhle*, in: Dürig/Herzog/Scholz, GG, 99. EL, September 2022, Art. 74 Rn. 120.
[17] Kritisch hierzu *Bäcker*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel B, Rn. 205 m.w.N.

Frage 7: Ist es aus dem Grundrecht auf informationelle Selbstbestimmung geboten, dass der Beschuldigte nach Abschluss einen Strafverfahrens darüber in Kenntnis gesetzt wird, ob und in welchem Umfang seinen Daten polizeilich gespeichert bleiben oder gelöscht werden?

Ja, es ist geboten, den Beschuldigten nach Abschluss eines Strafverfahrens darüber in Kenntnis zu setzen, ob und in welchem Umfang seine Daten polizeilich gespeichert bleiben oder gelöscht werden. Das Recht auf informationelle Selbstbestimmung ist nicht nur ein Abwehrrecht gegen staatliche Datenerhebung und -verarbeitung, sondern schützt auch das Interesse des Einzelnen, von staatlichen informationsbezogenen Maßnahmen zu erfahren, die ihn in seinen Grundrechten betreffen.[18] Die Kenntnis staatlicher Datenverarbeitung ist notwendige Voraussetzung, um gerichtlichen Rechtsschutz in Anspruch zu nehmen. Aber auch darüber hinaus gewährt das Recht auf informationelle Selbstbestimmung jedem Einzelnen das Recht, zu wissen, „*wer was wann und bei welcher Gelegenheit über* [ihn] *weiß*"[19]. Andernfalls können Einschüchterungseffekte eintreten und den Einzelnen in der freien Entfaltung seiner Persönlichkeit sowie in der Ausübung seiner Grundrechte einschränken.[20] Das Recht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[21]

Das Bundesverfassungsgericht führt dazu aus[22]: „*Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden (vgl. BVerfGE 65, 1 [43]). Nur wenn der Einzelne, der möglicherweise von einem Eingriff in das Recht auf informationelle Selbstbestimmung betroffen ist, eine Möglichkeit hat, von diesem Eingriff zu erfahren, kann er* die *für die freie Entfaltung seiner Persönlichkeit wichtige Orientierung und Erwartungssicherheit erlangen. Eine Informationsmöglichkeit für den von einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung*

[18] BVerfGE 120, 351, 360.
[19] BVerfGE 65, 1, 43.
[20] BVerfGE 65, 1, 43.
[21] BVerfGE 65, 1, 43.
[22] BVerfGE 120, 351, 360 f.

Betroffenen ist ferner Voraussetzung dafür, dass er die Rechtswidrigkeit der Informationsgewinnung oder etwaige Rechte auf Löschung oder Berichtigung geltend machen kann. Insoweit ist der Anspruch auf die Kenntniserlangung ein Erfordernis effektiven Grundrechtsschutzes im Bereich sowohl des behördlichen als auch des gerichtlichen Verfahrens (vgl. BVerfGE 100, 313 [361]; 109, 279 [363 f.])."

Frage 8: Ist es für einen effektiven Rechtsschutz geboten, dass die öffentliche Verwaltung im Land NRW eine Zentralstelle einrichtet, die dem Beschuldigten zur Auskunft über die gespeicherten Daten/Löschung von Daten nach Abschluss einen Strafverfahrens verpflichtet ist und der gegenüber ein Löschungsanspruch besteht und auch durchgesetzt werden kann?

Wichtig ist, dass Beschuldigte zuverlässig Auskunft über die zu seiner Person gespeicherten Daten erhält und mittels effektiven Rechtsschutzes einen eventuellen Löschungsanspruch durchsetzen kann. Dazu ist die Einrichtung einer Zentralstelle nicht zwingend erforderlich oder geboten. Dasselbe Ziel lässt sich auch auf anderem Wege erreichen. Ein wichtiger erster Schritt wäre die umfassende Sensibilisierung sämtlicher datenspeichernden Stellen der Verwaltung. Wenn selbst die Datenschutzbeauftragte berichtet, dass sie Probleme hat, ihre Kontrollaufgabe zu erfüllen, weil einzelne Behörden ihr die Kooperation verweigern,[23] sollte man eher dort ansetzen. Eine Zentralstelle hätte vermutlich dieselben Probleme. Statt eine Zentralstelle einzurichten, wäre die Übertragung der genannten Aufgaben auf die Datenschutzbeauftragte denkbar. Zudem sollte innerhalb jeder Behörde – sofern noch nicht geschehen – gem. § 5 Abs. 1 BDSG ein Datenschutzbeauftragter ernannt werden, der/die als Ansprechpartner bei Löschungsbegehren zur Verfügung steht.

Frage 9: Wie gehen andere Bundesländer mit der Frage der Sicherstellung der Löschung von Daten durch die Justiz um?

Zu dieser Frage habe ich keine weitergehenden Informationen als der Landtag Nordrhein-Westfalen. Die Landesdatenschutzbeauftragten der anderen Bundesländer könnten hierüber eventuell Auskunft geben.

[23] LDI NRW, 27. Bericht 2022, S. 54.

Frage 10: „Der Leitende Oberstaatsanwalt in Kleve wies darauf hin, dass die Staatsanwaltschaften gegenüber den Polizeibehörden keine Anordnungskompetenz hinsichtlich der dortigen polizeilichen Informationssysteme haben" (Bericht des Ministeriums der Justiz vom 20.03.2023 – Vorlage 18/1027 –, Seite 6, 2. Absatz). Wie bewerten Sie diese Einschätzung?

Polizeiliche und staatsanwaltschaftliche Informationssysteme sind grundsätzlich voneinander getrennt (Ausnahme: gemeinsame Dateisysteme i.S.d. § 486 StPO) und folgen jeweils unterschiedlichen Regeln. Das bringt der Bundesgesetzgeber zum Ausdruck, indem er an mehreren Stellen polizeiliche Datenbanken und Informationssysteme von den Regelungen der §§ 483 ff. StPO ausnimmt und sie jeweils landesgesetzlichen Regelungen des Polizeirechts überantwortet (z.B. in § 483 Abs. 1 S. 2, Abs. 3, § 484 Abs. 4, § 485 S. 4 StPO). Die Polizei kann nach Landesrecht personenbezogene Daten – etwa für Zwecke der Gefahrenabwehr – unter Umständen länger speichern als die Staatsanwaltschaft. Eine Anordnungsbefugnis scheidet daher bereits aus diesem Grund aus, denn die Datenspeicherung ist anders als das strafverfahrensrechtliche Ermittlungsverfahren keine untrennbare Einheit. Jede Behörde – und innerhalb der Behörde die Behördenleitung – ist vielmehr selbst für die Pflege ihrer Informationssysteme verantwortlich. Die Staatsanwaltschaft hat es aber in der Hand, die Polizei durch Übermittlung der notwendigen Informationen in die Lage zu versetzen, über die Datenlöschung zu entscheiden. Dazu ist es erforderlich, dass Mitteilungen des Verfahrensausgangs nach Nr. 11 Abs. 2 MiStra stets erfolgen und nicht nur dann, wenn der zuständige Staatsanwalt zufällig daran denkt. Eine wertvolle Hilfestellung ist daher die Voreinstellung im Textverarbeitungssystem ACUSTA. Eine automatisierte Versendung der Mitteilung wäre darüber hinaus eine große Arbeitserleichterung und würde sicherstellen, dass die Daten gelöscht werden.

Innerhalb der jeweiligen Behörden wäre die Kontrolle der Einhaltung der Löschungs- bzw. Aussonderungsprüffristen – ggf. nach Aufforderung durch das Datenverarbeitungsprogramm – durch den behördeneigenen Datenschutzbeauftragten zu erwägen (siehe Frage 5).

Mit freundlichen Grüßen

Tanja F. Niedernhuber

Dr. Tanja Niedernhuber