Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 14.02.2019

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur Anhörung im Rechtsausschuss des Deutschen Bundestages
am 20.02.2019
zum

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679

BT-Drucksache 19/4671

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Zur Änderung der Strafprozessordnung (Artikel 1)

Der Entwurf will die JI-Richtlinie umsetzen. Insoweit beschränkt er sich im Wesentlichen auf redaktionelle Änderungen. Er ändert aber darüber hinausgehend Befugnisse der Strafverfolgungs- und Sicherheitsbehörden, personenbezogene Daten zu verarbeiten, ohne dass dies durch die Richtlinie bedingt ist. Dies ist aus datenschutzrechtlicher Sicht abzulehnen. Daraus ergeben sich folgende Kritikpunkte, die in der nachfolgenden Stellungnahme im Detail dargestellt werden.

- Das Bundesverfassungsgericht (BerfG) hat in seiner Entscheidung zum Bundeskriminalamtgesetz (BKAG) festgelegt, nach welchen Maßgaben Daten aus heimlichen Ermittlungsmaßnahmen zu verarbeiten sind. Dies greift der Gesetzentwurf nicht für alle eingriffsintensiven Maßnahmen auf.
- Die in § 161 StPO-E vorgesehenen strikten Löschungsregeln gefährden eine ausreichende Möglichkeit zur Datenschutzkontrolle.
- Die Regelung in § 479 Abs. 2 S. 2 Nr. 2 StPO-E zur Übermittlung an die Nachrichtendienste ist zu unbestimmt und enthält keine ausreichenden Schwellen.
- Die Regelung in § 483 StPO-E greift intensiv in das Regelungssystem für die polizeiliche Datenverarbeitung ein. Er enthält kaum näher bestimmte tatbestandliche Einschränkungen zu Inhalt und Dauer der Speicherungen. Außerdem werden die Speicherschwellen des BKAG unterlaufen.
- Der Verweis in § 485 Satz 4 StPO-E ist abzulehnen. Regelungen im Bundeskriminalamtgesetz zur Datenverarbeitung schließen die hier vorgesehene Vermischung der Verarbeitungszwecke aus systematischen Gründen und aus Gründen der Verhältnismäßigkeit aus.
- Die in § 489 Abs. 5 StPO-E geregelte sogenannte „Mitziehautomatik“ ist abzulehnen. Eine entsprechende Regelung im Entwurf des BKAG wurde im parlamentarischen Verfahren gestrichen.

1. Fehlende Umsetzung

a) V-Personen:

Das BVerfG hat zuletzt mit seinem Urteil zum BKAG vom 20. April 2016 ein Grundsatzurteil zur Verarbeitung von Daten aus heimlichen Ermittlungsmaßnahmen getroffen (1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1681). Dies sind nach dem Urteil auch Erkenntnisse, die mit Hilfe von V-Personen ermittelt wurden. Das Gericht hat deren Einsatz als schwerwiegenden Grundrechtseingriff eingestuft, der einer hinreichend normenklaren- und bestimmten Rechtsgrundlage bedarf (NJW 2017, 1681, 1790, Rn. 160). Der Strafprozessordnung fehlt eine entsprechende Rechtsgrundlage, die eine Datenerhebung auf diesem Wege ermöglicht (vgl. dazu etwa Nr. 2.2. der

Anlage D zur RiStBV; Günther in: Münchener Kommentar zur StPO, 1. Auflage 2014, § 110a Rn. 28 m.w.N.; Frister in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Auflage 2018, Kap. F Rn. 328). Zwar konnte die bisherige Praxis noch auf die Rechtsprechung der Strafgerichte gestützt werden. Angesichts der verfassungsrechtlichen Rechtsprechung wird dies dauerhaft jedoch nicht aufrecht zu erhalten sein.

Daraus ergeben sich auch Probleme, wenn über V-Leute ermittelte Daten aus polizeilichen oder nachrichtendienstlichen Zusammenhängen in den Strafprozess eingeführt werden sollen. Dies gilt sowohl für Beweismittel als auch für Anknüpfungstatsachen. Verlangt man mit dem BVerfG nach dem sog. Doppeltürmodell neben der Übermittlungsregelung im jeweiligen Fachrecht auch eine entsprechende Erhebungsgrundlage auf der Empfängerseite (vgl. auch BVerfG NJW 2012, 1419, 1423, Abs. Nr. 320), dann fehlt es hieran auf Seiten der Strafverfolgungsbehörden. Nach dem Grundsatz der hypothetischen Datenneuerhebung darf die Strafverfolgungsbehörde zweckändernd Daten aus anderen Zusammenhängen nur erheben, wenn sie die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erheben dürfte (vgl. BVerfG NJW 2016, 1781, 1802, Abs. Nr. 287).

b) Kontrollbefugnisse

Die datenschutzrechtliche Kontrolle richtet sich nach den Vorschriften des Bundesdatenschutzgesetzes. Diese ist verfassungsrechtlich aufgrund der häufig heimlichen Datenverarbeitung zwingend (vgl. BVerfG NJW 2016, 1781, 1788, Rn. 135 m.w.N.). Artikel 47 Abs. 2 der JI-Richtline verpflichtet die Mitgliedstaaten, ausreichende Abhilfebefugnisse für die datenschutzrechtliche Aufsichtsbehörde vorzusehen. Bereits bei der Anhörung zum Bundesdatenschutzgesetz habe ich darauf hingewiesen, dass die in § 16 Abs. 2 BDSG vorgesehenen Abhilfebefugnisse nicht ausreichen. Formelle Beanstandungen führen in der Praxis nicht immer dazu, dass die betroffenen Behörden die Datenverarbeitung einschränken oder ändern. Lediglich in § 69 Abs. 2 BKAG sind über die Beanstandung hinausgehende Befugnisse festgelegt. Diese gelten aber für den Bereich der StPO dann nicht. Das ist nicht nur ein Wertungswiderspruch, sondern verstößt gegen die Vorgaben des Art. 47 Abs. 2 der JI-Richtlinie.

2. zu Artikel 1 Nr. 16 (§ 161 StPO-E)

a) zu Absatz 2:

Die Vorschrift enthält strikte Löschungsregeln für bestimmte besonders angeordnete Fälle. Das ist auf der einen Seite zu begrüßen, gefährdet aber auf der anderen Seite eine ausreichende Möglichkeit zur Datenschutzkontrolle. Namentlich schließt die Sonderregelung aus, Daten wegen schutzwürdiger Interessen der betroffenen Per-

son zu sperren (§ 58 Abs. 3 Nr. 1 BDSG). Die Daten können lediglich für den Fall einer gerichtlichen Überprüfung gesperrt werden. Wendet sich der Betroffene an die zuständige Datenschutzbehörde, kann diese nach der Neuregelung nicht mehr die Einschränkung der Verarbeitung anordnen, um der Eingabe mit einer datenschutzrechtlichen Kontrolle nachgehen zu können. Im Gegenteil kann die geprüfte Stelle eine datenschutzrechtliche Kontrolle sogar verhindern, wenn die Daten löschungsreif sind. Gerade für rechtswidrig verarbeitete Daten kann sich eine solche Löschungspflicht ergeben, weshalb die durchgehend sichergestellte datenschutzrechtliche Kontrolle hier besonders wichtig ist.

Gemäß Art. 16 Abs. 4 JI-RL muss zwingend eine aufsichtsbehördliche Prüfung möglich sein. Die Notwendigkeit der durchgehenden datenschutzrechtlichen Kontrolle ergibt sich auch aus den Anforderungen des BVerfG in seinem Urteil zum BKAG. Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen (BVerfG NJW 2016, 1781, 1789, Rn. 141).

Daher ist § 161 Absatz 2 Satz 2 StPO-E wie dargelegt entsprechend zu korrigieren.

b) Zu Absätzen 3 und 4:

Absatz 4 lässt Ausnahmen zur Nutzung als Ermittlungsansätze zu. Sofern die Daten aus Maßnahmen stammen, die einen Straftatenkatalog vorsehen (wie z.B. § 100a StPO), sollen diese nach der Gesetzesbegründung auch zur Aufklärung von Nicht-Katalogtaten verwendet werden dürfen „soweit diese jedenfalls vergleichbar bedeutend sind wie die im Katalog aufgeführten Taten“ (BT-Drs. 19/4671 S. 62). Damit dürfen TKÜ-Erkenntnisse im Ergebnis auch für die Verfolgung von Straftaten genutzt werden, die nicht im Katalog des § 100a StPO enthalten sind. Ob diese Erweiterung dem Geist des Urteils zum BKAG entspricht, darf bezweifelt werden. Der Gesetzgeber hat etwa in § 100a Abs. 2 StPO einen weiten Katalog definiert. Daneben noch weitere gleich „bedeutende“ (das BVerfG spricht hingegen von „gewichtigen“) Straftaten zu finden, führt zu unnötiger gesetzgeberischer Ungenauigkeit.

Ebenso wird die Formulierung des Absatzes 3 „ohne Einwilligung der Betroffenen Person“ kritisiert. Diese Formulierung lässt den Umkehrschluss zu, dass mit Einwilligung der betroffenen Person Datenverarbeitungen zulässig sind, für die eigentlich ein Verwertungsverbot gilt (Petri ZD 2018, 389). Grundlage der Datenverarbeitung ist dann die Einwilligung. Art. 8 Abs. 1 der JI-Datenschutzrichtlinie sieht die Einwilligung als Legitimationsgrundlage für eine Verarbeitung personenbezogener Daten durch Strafverfolgungsbehörden nicht vor. Dies ist im JI-Bereich anders geregelt als in Artikel 6 Absatz 1 Buchst. a DSGVO. Daher wird vorgeschlagen, statt der Einwilligung in § 161 Abs. 3 StPO-E den Antrag der betroffenen Person vorzusehen (siehe dazu im Einzelnen Petri a.a.O.).

3. zu Artikel 1 Nr. 24 (§ 477 bis 480 StPO-E)

a) zu § 479 Abs. 2 Satz 2 Nr. 3 StPO-E (Übermittlung an Nachrichtendienste)

Die Vorschrift ist **zu unbestimmt** und enthält keine ausreichenden Schwellen für die Übermittlung an die Nachrichtendienste. Im Übrigen ist bereits der Verweis ungenau, da § 18 BVerfSchG sechs Absätze hat, die größtenteils nicht die Strafverfolgungsbehörden betreffen.

Übermittlungsschwelle sind gemäß § 18 Abs. 1b S. 1 BVerfSchG lediglich „tatsächliche Anhaltspunkte dafür (…), dass die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist." Das BVerfG hat Übermittlungsvorschriften, die das informationelle Trennungsprinzip berühren, als nicht ausreichend angesehen, wenn diese lediglich darauf abstellen, ob die Übermittlung für die Aufgabenerfüllung erforderlich ist (BVerfG NJW 2013, 1499, 1505 und 1518, Rn. 126 und 232). Die Neuregelung des § 18 BVerfSchG ist daher verfassungsrechtlich kritisch zu sehen (ausführlich Bergemann in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Auflage 2018, Kap. H Rn. 119a). Daher ist auch der pauschale Verweis auf diese Vorschrift in § 479 Abs. 2 Nr. 3 StPO abzulehnen.

Besonders zweifelhaft ist dabei, dass für Übermittlungen nach § 18 BVerfSchG der Grundsatz der hypothetischen Datenneuerhebung offenbar gerade nicht gelten soll, abgesehen von den in § 479 Absatz 3 StPO-E genannten Maßnahmen. Denn dieser Grundsatz ist nur durch § 479 Absatz 2 Satz 1 StPO-E erfasst. Die Übermittlungen nach § 479 Absatz 2 Satz 2 Nummer 3 StPO-E sollen jedoch *„darüber hinaus"* zulässig sein.

b) zu § 479 Abs. 2 Satz 3 StPO-E

Die Löschungsregelung ist auch hier strikt formuliert. Es fehlt eine Einschränkung für Zwecke der Datenschutzkontrolle (siehe oben 2.b, zu Artikel 1 Nr. 16, § 161 StPO-E).

4. zu Art. 1 Nr. 27 (§ 483 StPO-E)

Die geplante Vorschrift greift intensiv in das Regelungssystem für die polizeiliche Datenverarbeitung ein. Die Änderung hat eine erhebliche inhaltliche Tragweite.

Dort, wo das polizeiliche Datenschutzrecht derzeit noch Grenzen setzt, kann der geplante § 483 StPO-E künftig wie ein Generalschlüssel wirken, mit dem auch Unbeteiligte, Zeugen etc. in die Informationssysteme fließen, obwohl sie gemäß § 16 Abs. 5

Nr. 2 i.V.m. § 18 BKAG eigentlich nicht im Informationssystem gespeichert werden dürften.

Betroffen kann jeder sein.

Damit verzichtet der Entwurf zudem darauf, den Kreis der betroffenen Personen gemäß Artikel 6 der JI-Richtlinie zu konkretisieren.

a) Bereits vorhandene Reichweite der gegenwärtigen Vorschrift

§ 483 StPO-E enthält **kaum näher bestimmte tatbestandliche Einschränkungen zu Inhalt und Dauer der Speicherungen**. Eine umfangreiche Speicherung kann lediglich dann gerechtfertigt sein, wenn sie sich auf ein bestimmtes Strafverfahren beschränkt. Zweck des noch geltenden § 483 StPO ist es ***bislang***, die elektronische Auswertung umfangreichen Beweis- oder Hinweismaterials **innerhalb eines bestimmten Strafverfahrens** zu ermöglichen. Dafür verzichtet § 483 StPO auf näher bestimmte Grenzen. Er erlaubt eine umfassende Speicherung, ohne den Inhalt, die Dauer, den Umfang und die Möglichkeiten der Auswertung näher zu benennen. Es kommt danach lediglich auf die Erforderlichkeit „für Zwecke des Strafverfahrens“ an.

Damit ist § 483 StPO die zentrale Vorschrift, um etwa umfangreiche Beweismittel und Spuren aus großen Verfahren zu verarbeiten. In der Praxis können solche Dateien beispielsweise die Daten aus Rasterfahndungsmaßnahmen oder Funkzellendatenauswertungen enthalten. Beides kann die Daten zu vielen Millionen **unbeteiligten Personen** bzw. **Zeugen** umfassen. Solche Dateien können zudem Informationen zu durch die Straftat **geschädigten Personen** enthalten. Hierbei kann es sich um besonders **sensible Informationen** handeln, wie etwa bei Sexualstraftaten. Ebenfalls können Geschäfts- und Betriebsgeheimnisse umfasst sein.

Das wirft verfassungsrechtlich und im Hinblick auf Artikel 6 der JI-Richtlinie durchaus Fragen auf. Es ist nur dann zu rechtfertigen, wenn die Strafverfolgungsbehörde sich – entsprechend dem Wortlaut der bisherigen Regelung – darauf begrenzt, in einer „bestimmten“ Datei – also einem **logisch abgegrenzten Bereich der IT-Systeme** – nur die Daten für ein „bestimmtes“ Strafverfahren zu speichern. Das schließt Dateien aus, in denen verfahrensübergreifend alle Daten aus allen Strafverfahren gesammelt werden.

Genau um diese Frage geht es aber in den Diskussionen aus der bisherigen Praxis (siehe BfDI, 26. Tätigkeitsbericht, Nr. 10.2.9.3, Zentralstellen- und Strafverfolgungsdateien beim BKA).

b) Voraussetzungslose Speicherungen, Unterlaufen der polizeirechtlichen Grenzen

Künftig sollen nach dem neuen § 483 Absatz 1 Satz 2 StPO-E die Daten in die Informationssysteme der Polizeibehörden fließen. Anders als bei Justizbehörden spricht die Neufassung in § 483 Abs. 1 S. 2 StPO-E nicht mehr von (begrenzten) „Dateien“, sondern von (wenig begrenzten) „Informationssystemen“. Für diesen Zweck sind die Informationssysteme der Polizeibehörden aber gerade nicht gedacht. Das Informationssystem des BKA ist vielmehr der grundlegende Informationsbestand, mit dem das BKA am Informationsverbund der Polizeien des Bundes und der Länder teilnimmt und auch hausintern für eine **breite Streuung der Informationen** sorgt (§ 13 Abs. 3 BKAG). Aus dieser Funktion entspringt der Name „Informationssystem“. Um das System verhältnismäßig zu halten, ist der zu speichernde Personenkreis gemäß § 18 BKAG beschränkt. Das Informationssystem dient der vorbeugenden Gefahrenabwehr. Hingegen ist es nicht darauf angelegt, einzelne Verfahren zu „bearbeiten“. Zu Informationssystemen der Bundespolizei und der Zollfahndung bestehen noch keine Rechtsvorschriften. Die Ländervorschriften können sehr unterschiedlich ausgestaltet sein. Zur Reichweite und den Auswirkungen der auch im BKAG neu gefassten Vorschriften zum Informationssystem des BKA habe ich im Gesetzgebungsverfahren zur Neustrukturierung des BKAG ausführlich Stellung genommen (A-Drs. 18(4)806 A).

Haben Polizeibehörden Daten in einem Strafverfahren erhoben und stützen sie sich auf § 483 StPO, soll § 18 BKAG offenbar nicht gelten. Der neu eingefügte § 483 Abs. 1 Satz 2 StPO-E **unterläuft** damit die **Speicherschwellen** des BKAG. Damit besteht die Gefahr, dass die nach § 483 StPO gespeicherten Daten zu multifunktionalen Zwecken in die Informationssysteme diffundieren. Denn die Datenbestände sind nicht voneinander getrennt. Errichtungsanordnungen oder Regelungen zur Kennzeichnung und Zugriffsbeschränkung greifen nicht.

- *Beispiel*: *Im Strafverfahren gegen einzelne Mitgesellschafter und verschiedene Mitarbeiter der Wirtschaftsprüfungsgesellschaft „W Partnerschaft“ werden umfangreiche Datenmengen, Geschäfts- und Mandantenunterlagen beschlagnahmt. Diese befinden sich auf Datenträgern und in Akten, die für das Strafverfahren zu großen Teilen eingescannt werden. Wie bislang soll die elektronische Erfassung dazu dienen, die Auswertung des Beweismaterials mit Analysesoftware zu erleichtern und zu ermöglichen. In den beschlagnahmten Daten befinden sich umfangreiche Informationen über die Mandanten der Wirtschaftsprüfungsgesellschaft. Die Speicherung der Daten zu Mandanten im Informationssystem wäre nach § 18 BKAG unzulässig, da gegen sie überwiegend kein Verdacht besteht. Über § 483 StPO-E, der den Personenkreis und die Voraussetzungen der Speicherung nicht begrenzt, werden die Daten vollständig im Informationssystem gespeichert. Auch die Kundendaten stehen nun im polizeilichen Informationsbestand zur Verfügung und sind mit Analysemitteln auswertbar und können mit weiteren Daten etwa zu Ereignissen der Gefahrenabwehr oder Strafverfolgung verknüpft werden. Die Polizeibehörde*

stellt sich auf den Standpunkt, dies sei nicht auf das konkrete Strafverfahren begrenzt.

Errichtungsanordnungen sieht das bestehende BKAG – entgegen meiner nach wie vor gültigen Kritik – nicht mehr vor. Offenbar soll auch der neue § 483 Abs. 1 S. 2 StPO-E zu einem Verzicht auf die Errichtungsanordnungen führen, soweit die Daten in einem Informationssystem gespeichert sind. Damit ist auch für das Strafverfahren insoweit nicht mehr genau festzulegen, für welches Verfahren die Daten gespeichert sind und welchen Zwecken die Speicherung dient.

Diese fehlenden Begrenzungen und Unklarheiten werden nicht durch die Kennzeichnungs- und Zugriffsregelungen kompensiert. Denn nach § 15 BKAG ist für die Vergabe der Zugriffsrechte maßgeblich, wie die Daten nach § 14 BKAG gekennzeichnet sind. Nach § 14 Abs. 1 BKAG ist aber **lediglich zu kennzeichnen, mit welchem *„Mittel“* die Daten erhoben wurden** (nicht notwendig die Rechtsgrundlage der Erhebung, arg. e contrario aus § 14 Abs. 1 S. 2 BKAG). Ebenso ist zu kennzeichnen, welcher Personenkategorie die Personen zuzuordnen sind, soweit zu ihnen Grunddaten angelegt worden sind (Personenkategorien sieht § 483 StPO nicht vor!). Ferner ist die (abstrakte) Angabe der geschützten Rechtsgüter oder der verfolgten Straftaten erforderlich. **§ 14 BKAG schreibt hingegen *nicht* vor, die Rechtsgrundlage der Speicherung des jeweiligen Datums zu kennzeichnen.** Insbesondere sieht § 14 BKAG nicht vor, zu kennzeichnen, dass Daten nach § 483 StPO für „Zwecke des Strafverfahrens“ – also für ein ***bestimmtes*** Strafverfahren (Wittig in: BeckOK StPO, 29. Edition, Stand: 01.01.2018, § 483 Rn. 1) – gespeichert sind. Auch der in § 15 BKAG erwähnte § 12 BKAG umschreibt lediglich die allgemeinen Aufgaben des BKAG im Hinblick auf eine zweckändernde Verwendung, nicht aber den konkreten Zweck der Speicherung. Das BKAG geht insoweit davon aus, dass die Daten im Informationssystem immer nach den Vorschriften des BKAG selbst gespeichert sind. Daher passt sich die geplante Regelung in § 483 Absatz 1 Satz 2 StPO-E auch systematisch nicht ein.

Ob in der datenschutzrechtlichen Kontrollpraxis später nachvollzogen werden kann, auf welcher Grundlage die Daten im Informationssystem gespeichert sind, ist deshalb in § 483 Absatz 1 Satz 2 StPO offen gelassen.

Damit enthält eine Speicherung gemäß § 483 StPO aufgrund der neu vorgesehenen Änderung praktisch keinerlei tatbestandliche Grenzen mehr.

Im Ergebnis diffundieren die nach § 483 StPO gespeicherten Daten mit den für Zwecke der Gefahren- bzw. Strafverfolgungsvorsorge gespeicherten Daten im Informationssystem. Sie sind dann – auch mit Mitteln der Kombination und Analyse - multifunktional auswertbar. Auch die Namen der Mandanten in dem dargestellten Beispiel

und weitere persönliche Informationen zu ihnen können dann in Charts und Metadatenanalysen umfangreich verwendet werden, solange dies nur derselben Aufgabe oder einem allgemein zulässigen Zweck gemäß § 12 BKAG dient. § 18 BKAG, der dies auf einen bestimmten Personenkreis begrenzt, der hinreichend Anlass für solche Auswertungen gegeben hat, wird damit unterlaufen.

c) Regelungsvorschlag

In den Gesetzeswortlaut sollte daher nach § 483 Abs. 1 Satz 2 StPO-E mindestens folgender Satz 3 eingefügt werden:

> *„Die Verarbeitung erfolgt in einem für das jeweilige Strafverfahren durch Zugriffsbeschränkungen abgegrenzten Bereich des Informationssystems."*

5. zu Artikel 1 Nr. 29 Buchst. b (§ 485 StPO-E)

Der Verweis in § 485 Satz 4 StPO-E ist abzulehnen. Im Informationssystem gemäß § 16 BKAG ist die Vorgangsverwaltung nicht vorgesehen. Vielmehr ist diese in § 22 Abs. 2 BKAG vorgesehen. Danach ist die Datenverarbeitung dann auf die Vorgangsverwaltung und die befristete Dokumentation polizeilichen Handelns begrenzt („ausschließlich zu diesem Zweck"). Das schließt die in § 485 Satz 4 StPO-E vorgesehene Vermischung der Verarbeitungszwecke aus systematischen Gründen und aus Gründen der Verhältnismäßigkeit aus.

6. zu Artikel 1 Nr. 33 (§ 489 StPO)

Die in § 489 Absatz 5 StPO-E (Abs. 6 a.F.) geregelte **sogenannte „Mitziehautomatik"** ist abzulehnen, auch soweit sie in Zukunft nur Beschuldigte betrifft. Sie führt zu unabsehbar langen Dauerspeicherungen, ohne im Einzelfall die Verhältnismäßigkeit hinreichend sicherzustellen. Sie gilt unabhängig von der Schwere der Vorwürfe und der Sachzusammenhänge. So kann nach einer eigentlich beendeten „kriminellen Karriere" auch ein leichtes Fahrlässigkeitsdelikt nach einem Verkehrsunfall alte Speicherungen mitziehen. Sie verstößt gegen Art. 7 Abs. 2 der JI-Richtlinie.

Die Vorschrift stellt nicht auf den Einzelfall ab, sondern lässt – ohne die Gründe im Einzelfall überhaupt zu berücksichtigen – pauschal die Speicherung älterer Sachverhalte zu, wenn ein neuer Sachverhalt hinzutritt. Dies betrifft auch solche älteren Speicherungen, bei denen die betroffene Person nur aufgrund einer vagen Verdachtsspeicherung erfasst ist und ggf. „aus Mangel an Beweisen" freigesprochen oder das Verfahren aus diesen Gründen eingestellt wurde und zudem auch Bagatelldelikte. Es ist aber schlicht nicht erforderlich, z.B. den vagen Verdacht eines Diebstahls geringwertiger Sachen zu speichern, der 25 Jahre in der Vergangenheit liegt.

Der Vorschlag, eine entsprechende Regelung auch für den Bereich polizeilicher Verbunddateien zu schaffen, wurde zum BKAG im parlamentarischen Verfahren aus zutreffenden Gründen abgelehnt (vgl. BT-Drs. 18/12076 und BT-Drs. 18/12141 Nr. 1 Buchst. q). Zur weiteren Begründung verweise ich auf meine Stellungnahme zum BKAG, A-Drs. 18(4)806A, S. 11ff. [1]).

Zwar spielt § 489 StPO in der Praxis bislang keine nennenswerte Rolle, da aufgrund der Kollisionsregel vorrangig Polizeirecht gilt. Im Bereich der Staatsanwaltschaften erreichen die Vorsorgedatenbanken nicht denselben Umfang, der der polizeilichen Datenspeicherung vergleichbar ist. Gleichwohl ergeben sich dieselben prinzipiellen Bedenken, wie im Bereich des Polizeirechts.

§ 489 Absatz 5 StPO-E sollte ersatzlos **gestrichen werden**.

7. zu Artikel 1 Nr. 41 (§ 500 StPO)

Von Seiten der Länder werden teilweise Unsicherheiten befürchtet, die durch den neuen § 500 StPO entstehen. Dort wird für den Bereich der Strafverfolgungsbehörden vollständig auf die ergänzende Anwendung des Bundesdatenschutzgesetzes verwiesen. Die Strafverfolgungsbehörden sind aber größtenteils Landesbehörden. Soweit die Polizeibehörden nach der StPO handeln würde dann ergänzend das BDSG gelten, soweit sie nach Polizeirecht handeln, das jeweilige Landesdatenschutzgesetz. Probleme könnten etwa dann entstehen, wenn für automatisierte Systeme unterschiedliche Standards gelten.

Vor allem ist unklar, welche Befugnisse den Landesbeauftragten zustehen. Die Befugnisse des BfDI sind in Teil 1 des BDSG geregelt, die der Landesbeauftragten nicht. Zur Reichweite der Befugnisse siehe oben 1.b.

[1] https://www.bundestag.de/blob/497658/a9b614f915a568e32a2b5d87cf4acdbf/18-4-806-a-data.pdf