19. Wahlperiode

Deutscher Bundestag

Ausschuss für Recht und Verbraucherschutz

Wortprotokoll
der 37. Sitzung

Ausschuss für Recht und Verbraucherschutz
Berlin, den 20. Februar 2019, 15:01 Uhr
Berlin, Paul-Löbe-Haus, Saal E.800

Vorsitz: Stephan Brandner, MdB

Tagesordnung - Öffentliche Anhörung

Einziger Tagesordnungspunkt **Seite 14**

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-Drucksache 19/4671

Federführend:
Ausschuss für Recht und Verbraucherschutz

Mitberatend:
Ausschuss für Inneres und Heimat
Ausschuss Digitale Agenda

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Axel Müller [CDU/CSU]
Abg. Dr. Johannes Fechner [SPD]
Abg. Roman Johannes Reusch [AfD]
Abg. Dr. Jürgen Martens [FDP]
Abg. Niema Movassat [DIE LINKE.]
Abg. Canan Bayram [BÜNDNIS 90/DIE GRÜNEN]

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

Mittwoch, 20. Februar 2019, 15:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		CDU/CSU	
Frieser, Michael		Amthor, Philipp	
Heil, Mechthild		Frei, Thorsten	
Heveling, Ansgar		Gutting, Olav	
Hirte Dr., Heribert		Hauer, Matthias	
Hoffmann, Alexander		Launert Dr., Silke	
Jung, Ingmar		Lindholz, Andrea	
Luczak Dr., Jan-Marco		Maag, Karin	
Müller, Axel		Middelberg Dr., Mathias	
Müller (Braunschweig), Carsten		Nicolaisen, Petra	
Sensburg Dr., Patrick		Noll, Michaela	
Steineke, Sebastian		Schipanski, Tankred	
Ullrich Dr., Volker		Thies, Hans-Jürgen	
Warken, Nina		Throm, Alexander	
Wellenreuther, Ingo		Vries, Kees de	
Winkelmeier-Becker, Elisabeth		Weisgerber Dr., Anja	

15. Februar 2019

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

19. Wahlperiode

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 20. Februar 2019, 15:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
SPD		**SPD**	
Brunner Dr., Karl-Heinz		Esken, Saskia	
Dilcher, Esther		Högl Dr., Eva	
Fechner Dr., Johannes		Lischka, Burkhard	
Groß, Michael		Miersch Dr., Matthias	
Heidenblut, Dirk		Müller, Bettina	
Ryglewski, Sarah		Nissen, Ulli	
Scheer Dr., Nina		Özdemir (Duisburg), Mahmut	
Schieder, Marianne		Rix, Sönke	
Steffen, Sonja Amalie		Vogt, Ute	

15. Februar 2019

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

Seite 2 von 4

19. Wahlperiode

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 20. Februar 2019, 15:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
AfD		**AfD**	
Brandner, Stephan		Curio Dr., Gottfried	
Jacobi, Fabian		Hartwig Dr., Roland	
Maier, Jens		Haug, Jochen	
Maier Dr., Lothar		Seitz, Thomas	
Peterka, Tobias Matthias		Storch, Beatrix von	
Reusch, Roman Johannes		Wirth Dr., Christian	
FDP		**FDP**	
Buschmann Dr., Marco		Fricke, Otto	
Helling-Plahr, Katrin		Ihnen, Ulla	
Martens Dr., Jürgen		Schinnenburg Dr., Wieland	
Müller-Böhm, Roman		Skudelny, Judith	
Willkomm, Katharina		Thomae, Stephan	

15. Februar 2019

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz

Seite 3 von 4

19. Wahlperiode

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 20. Februar 2019, 15:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
DIE LINKE.		**DIE LINKE.**	
Akbulut, Gökay		Jelpke, Ulla	
Mohamed Ali, Amira		Lay, Caren	
Movassat, Niema		Möhring, Cornelia	
Straetmanns, Friedrich	F.K	Renner, Martina	
BÜ90/GR		**BÜ90/GR**	
Bayram, Canan		Kühn (Tübingen), Christian	
Keul, Katja		Künast, Renate	
Rößner, Tabea		Mihalic Dr., Irene	
Rottmann Dr., Manuela		Schauws, Ulle	
		K. v. Notz	

15. Februar 2019

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz

Seite 4 von 4

Sitzung des Ausschusses für Recht und Verbraucherschutz
(6. Ausschuss)
Mittwoch, 20. Februar 2019, 15:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
AFD		
FDP		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
Simolot	SPD	
Sparr	SPD	
Bick	FDP	
Stark	FDP	
Leopold	Grüne	
Gerig Raue	CDU	
Dr. Leonhardt	CDU/CSU	
Zell	LINKE	
Kriegel Irbe	CDU/CSU	

Stand: 13. September 2018 / ZT4, Luisenstr. 32-34, Telefon: +49 30 227-32659
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz
(6. Ausschuss)
Mittwoch, 20. Februar 2019, 15:00 Uhr

Fraktionsmitarbeiter

Name (bitte in Druckschrift)	**Fraktion**	Unterschrift
Jörn Pohl	Grüne	

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz
(6. Ausschuss)
Mittwoch, 20. Februar 2019, 15:00 Uhr

Bundesrat

Land	**Name** (bitte in Druckschrift)	**Unterschrift**	**Amtsbezeichnung**
Baden-Württemberg			
Bayern	Dr. Wegner		ORR
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen			
Mecklenburg-Vorpommern	Petermeier		RDir
Niedersachsen	BERTRANG		OStRin
Nordrhein-Westfalen			
Rheinland-Pfalz	Jacobi		RR
Saarland			
Sachsen			
Sachsen-Anhalt			
Schleswig-Holstein	Martens		RD
Thüringen			

Stand: 13. September 2018 / ZT4, Luisenstr. 32-34, Telefon: +49 30 227-32659
Es gelten die Datenschutzhinweise unter: https://www.bundestag.de/datenschutz.

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 20. Februar 2019, 15:00 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	Name (bitte in Druckschrift)	Unterschrift	Amtsbezeichnung
BMJV	Cai Rüffer		VtA
BMJV	Nikradzik, C.		MDn
BMJV	Peter, Martina		RDn
BMJV	Dr. Dörrbecker, Alexander		RD
BMJV	Dr. Paul Tophof		Referendar
BfDI	Dirk Hensel		RD
BfDI	Nics Bergemann		RD
BMI	Hagen Nollau		RR
BMJV	Dr. Becker, Monika		OStA BGH

Anwesenheitsliste der Sachverständigen

zur Anhörung des Ausschusses für Recht und Verbraucherschutz
am Mittwoch, 20. Februar 2019, 15.00 Uhr

Name	Unterschrift
Dr. Viktoria Bunge Ministerium für Justiz, Europa, Verbraucherschutz und Gleichstellung des Landes Schleswig-Holstein Staatsanwältin	
Dr. Georg Gieg Richter am Oberlandesgericht Bamberg	
Ria Halbritter Rechtsanwältin, Berlin	
Matthias Kegel Generalstaatsanwaltschaft des Landes Brandenburg Oberstaatsanwalt, IT-Dezernent	
Ulrich Kelber Bundesbeauftragter für den Datenschutz und die Informationsfreiheit	
Dr. Gerwin Moldenhauer Der Generalbundesanwalt beim Bundesgerichtshof Oberstaatsanwalt beim Bundesgerichtshof	
Prof. Dr. Thomas Petri Bayerischer Landesbeauftragter für den Datenschutz	
Dr. Lisa Kathrin Sander Generalstaatsanwaltschaft Frankfurt a. M. Oberstaatsanwältin	

Anwesenheit des Sachverständigen

Nils Bergemann	

nach Abwesenheit des Sachverständigen Ulrich Kelber.

Sprechregister Abgeordnete

Sprechregister Sachverständige

Der Vorsitzende **Stephan Brandner**: Meine Damen und Herren, ich begrüße Sie herzlich zur 37. Sitzung unseres Ausschusses, zur zweiten Sitzung am heutigen Tage. Es handelt sich um die öffentliche Anhörung zum Gesetzentwurf der Bundesregierung zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679. Ich begrüße herzlich die Abgeordneten hier im Kreise. Ich begrüße herzlich die heute acht Sachverständigen; sonst haben wir neun Sachverständige. Und ich begrüße auch Herrn Kelber herzlich – Sie kennen das hier ja auch als Staatssekretär von der anderen Seite, bevor Sie Bundesbeauftragter für den Datenschutz und die Informationsfreiheit geworden sind. Ich begrüße weiter herzlich die Vertreter der Bundesregierung. Staatssekretär Lange ist noch im Plenum und kommt gegebenenfalls später. Herr Kelber hat angekündigt, um 16.30 Uhr die Anhörung aufgrund eines anderen Termins verlassen zu müssen. Ein Vertreter wäre aber hier, der in der Sache dann ebenfalls Auskunft geben könnte. Ich begrüße auch die nicht allzu zahlreichen Besucher auf der Tribüne. Ich denke, heute kann ich die Belehrung kurz gestalten. Stören Sie bitte nicht von der Tribüne, machen Sie keine Fotos und twittern Sie bitte auch nicht. Auf der Grundlage einer Tonaufzeichnung wird später ein Wortprotokoll erstellt. Das Verfahren der Anhörung läuft wie üblich: Die Sachverständigen erhalten die Möglichkeit zu einer Eingangsstellungnahme von vier Minuten. Dort oben läuft eine Uhr rückwärts. Nach drei Minuten und dreißig Sekunden ertönt ein Signal, nach vier Minuten ebenfalls. Nach dem zweiten Signal sollten Sie langsam zum Ende kommen. Nach den Eingangsstellungnahmen gibt es die erste Fragerunde der Abgeordneten. Darauf folgt die entsprechende Antwortrunde. Möglicherweise schließen sich weitere Frage- und Antwortrunden an. Hinsichtlich der Reihenfolge der Redner gehen wir wie folgt vor: Wir beginnen bei den Eingangsstellungnahmen alphabetisch, heute mit „B“ und enden bei „S“. Bei der ersten Antwortrunde verfahren wir in entgegengesetzter Reihenfolge, beginnen bei „S“ und enden bei „B“. Die Reihenfolge wechselt dann bei jeder Antwortrunde. Die Abgeordneten kennen das bei uns übliche Verfahren: Danach hat jeder Abgeordnete das Recht, zwei Fragen zu stellen. Entweder zwei Fragen an einen Sachverständigen oder jeweils eine Frage an zwei Sachverständige. Das war das Wichtige, was ich einleitend zu sagen hatte. Dann kann Frau Bunge, wenn Sie bereit sind, mit der Eingangsstellungnahme beginnen. Bitte schön.

SVe **Dr. Viktoria Bunge**: Ich möchte meine Stellungnahme auf zwei Punkte beschränken, einmal zur Strafprozessordnung (StPO) und dann zum Strafvollzugsgesetz (StVollzG). Hinsichtlich der StPO habe ich drei Anmerkungen zu machen. Zum einen geht es um die zahlreichen Verweisungen auf das Bundesdatenschutzgesetz (BDSG) bzw. den generellen Verweis des § 500 des Entwurfes. Das ist in meinen Augen verbesserungswürdig und zwar aus zwei Punkten: Zum einen ist es so, dass das sehr, sehr anwenderunfreundlich ist, wenn man mehrere Male verweisen muss, wenn man hinschauen muss, welches Gesetz denn tatsächlich anwendbar ist, was ja dann sogar die Krux haben kann, dass man selbst im BDSG noch einmal verwiesen wird und dann möglicherweise auch noch in die Datenschutz-Grundverordnung (DSGVO) hineinschauen muss. Darüber hinaus beinhaltet das in meinen Augen das Problem, dass es dann auch zu divergierenden Entscheidungen kommen kann, weil der Gesetzentwurf ja vorsieht, dass die eine Reglung abschließend sein soll und in der anderen Regelung soll subsidiär auf das BDSG verwiesen werden. Das kann halt dazu führen, dass die Frage, ob eine Regelung der StPO abschließend ist, in der Praxis unterschiedlich beantwortet wird. Der zweite Punkt betrifft die Verarbeitung besonderer Kategorien von personenbezogenen Daten. Das sind beispielsweise Daten zur rassischen und ethnischen Herkunft oder Gesundheitsdaten. Nach Art. 10 der Richtlinie kann man diese nur verarbeiten, sofern das unbedingt erforderlich ist. In dem Gesetzentwurf findet sich ein Hinweis nur in § 161 StPO-E und dort wird wiederum auch nur auf § 48 BDSG verwiesen. Das führt in meinen Augen dazu, dass

es dann für die Praxis verwirrend wird, weil diese Grundlage der Verarbeitung besonderer personenbezogener Daten ja für alle Verarbeitungsvorgänge gilt, insbesondere auch zum Beispiel für die Übermittlung. Und auch da sollte man sich stets vor Augen führen, dass diese Daten nur übermittelt werden dürfen, wenn es unbedingt erforderlich ist. Der letzte Punkt zur StPO betrifft eine für mich auch in der Praxis sehr relevante Vorschrift, und zwar § 487 Abs. 1 Satz 3 StPO. Nach der geltenden Fassung ist es nämlich so, dass personenbezogene Daten vom Bewährungshelfer an den Justiz- und Maßregelvollzug zur weiteren Vollzugs- und Eingliederungsplanung nur übermittelt werden dürfen, wenn der Verurteilte, also der Proband, noch unter Aufsicht gestellt ist. Das bedeutet, wenn sozusagen schon ein rechtskräftiger Widerruf vorliegt, also keine Aufsicht mehr besteht, können diese Daten nicht übermittelt werden. Und gerade dann, wenn ein Widerruf vorliegt – das heißt, es ist zwingend dass er sozusagen wieder aufgenommen wird –, sind die Daten ja relevant, sodass wir in der Praxis bisher dann immer mit Schweigepflichtentbindungen arbeiten müssen, was ja das Prozedere erheblich verzögert und auch schwieriger macht.

Im zweiten Punkt möchte ich mich gerne den Regelungen des StVollzG widmen, und zwar dort vier Punkten. Meines Erachtens fehlt eine Regelung zum Akteneinsichtsrecht für die Mitglieder der Delegation des Ausschusses zur Verhütung von Folter, unmenschlicher und erniedrigender Behandlung oder Strafe (CPT). Und zwar ist es ja so, dass das StVollzG momentan primär einschlägig ist für Zivilgefangene und für den gerichtlichen Rechtsschutz und dass sich in den Strafvollzugsgesetzen und den Justizvollzugs-datenschutzgesetzen entsprechende Akteneinsichtsrechte befinden bzw. dass die Gesetzgeber im Begriff sind, entsprechende Regelungen zu schaffen. Und wenn es jetzt für Zivilgefangene keine Regelung gibt, führt das in der Praxis zu dem Problem, dass unsere Bediensteten oder Mitarbeiter nicht wissen, wenn denn der CPT mal kommt, ob dann diese Akten entsprechend herauszugeben sind. Darüber hinaus fehlt meines Erachtens ein Akteneinsichtsrecht für die Gesundheitsakten. § 185 StVollzG setzt die Entscheidung des Bundesverfassungsgerichts vom 20. Dezember 2016 nicht hinreichend um. Dort hatte das Bundesverfassungsgericht ja gesagt, dass aufgrund der Sensibilität und des schweren Eingriffs dieser Datenerhebung in diesem Bereich ein Auskunftsrecht der Gefangenen nicht ausreicht, sondern grundsätzlich ein Akteneinsichtsrecht zur Verfügung stehen muss. Und dem wird die Vorschrift in ihrer bisher geltenden Fassung bzw. in der Form, wie sie nun gefasst werden soll, meines Erachtens nicht gerecht.

Darüber hinaus möchte ich darauf hinweisen, dass es in vielen Landesstrafvollzugsgesetzen oder Justizvollzugsdatenschutzgesetzen spezielle Regelungen für erhebungs- und datenrechtliche Verarbeitungsvorgänge, wie beispielsweise das Auslesen von Datenspeichern, gibt. Das betrifft beispielsweise den Fall, in dem man ein Handy in einer Justizvollzugsanstalt gefunden hat, dass man dann unter gewissen Voraussetzungen die Möglichkeit hat, dieses auszulesen und die Daten unter gewissen – auch wieder einschränkenden – Voraussetzungen zu nutzen. Nun ist es so, dass wenn diese Regelung im StVollzG fehlt und man ein Handy bei einem Zivilgefangenen findet, nicht die Möglichkeit besteht, dieses auszulesen und sich anzuschauen. Und dann möchte ich noch ganz kurz auf § 88 StVollzG zu den besonderen Sicherungsmaßnahmen zu sprechen kommen. Meines Erachtens sollte auch insoweit eine Videoüberwachung möglich sein, nämlich bei Suizidgefahr.

Der **Vorsitzende**: Vielen Dank. Nun bitte die Ausführungen des Herrn Gieg. Bitte schön, Sie haben das Wort.

SV **Dr. Georg Gieg**: Vielen Dank. Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren Abgeordnete, sehr geehrte Damen und Herren! Zunächst einmal – und das möchte ich nicht vergessen, zu erwähnen – ist es für mich eine äußerst ehrenvolle Sache, dass ich heute hier vor dem Hohen Haus gehört werde. Das ist eine Premiere und eine außerordentliche Ehre für mich. Ich hab nach Kräften versucht, mich in der

außerordentlich kurzen Zeit einzuarbeiten, bitte aber um Verständnis dafür, dass ich im Wesentlichen den Blick auf das Strafprozessrecht richten will. Ich bin Revisionsrichter seit mehr als zehn Jahren und in Revisions- und Rechtsbeschwerdesachen in Bamberg tätig, da spielen diese Fragen meist keine Rolle. Meine Befassung rührt deshalb in erster Linie daher, dass ich als Bearbeiter eines Strafprozessrechtskommentars die Ehre habe, die hier uns interessierenden Vorschriften seit einigen Auflagen zu kommentieren. Auch wenn es vielleicht merkwürdig klingt, aber ich halte den Gesetzentwurf der Bundesregierung für einen mehr als beachtlichen und angesichts der Komplexität und des Umfangs der Aufgabe ganz überwiegend inhaltlich wie handwerklich gelungenen Entwurf. Die Schwierigkeit besteht ja nicht nur darin, das „neue Recht“ angesichts der gerade in der StPO gepflegten, mitunter anstrengenden Verweisungstechnik auf andere Bestimmungen desselben Gesetzes umzusetzen. Die StPO ist ja kaum mehr lesbar, selbst für einen Praktiker nicht mehr. Hinzu kommt, dass in dieses für den Normanwender ohnehin komplexe Geflecht die Anforderungen insbesondere der Richtlinie 2016/680 vom 27. April 2016 einzuweben sind, und dabei die neue DSGVO und mit dieser wiederum im Schlepptau das neue BDSG nicht aus den Augen zu verlieren sind. Dass der durchgängig mit spürbarer Vorsicht, ja Behutsamkeit begründete Entwurf dennoch im Wesentlichen als deutsches Verfahrensrecht wiedererkennbar bleibt, ist ebenso erfreulich wie die für die Akzeptanz des vorgesehenen Regelwerks nicht minder bedeutsame Umsetzung zentraler Anliegen der Rechtsprechung des Bundesverfassungsgerichts. So wird nach meiner Überzeugung etwa allein und unabhängig vom diskussionswürdigen Standort – wo ist es verortet im Gesetz – und weiteren Detailfragen die Verankerung des für eingriffsintensive Überwachungs- und Ermittlungsmaßnahmen vom BVerfG geforderten ausfüllenden Schranken-Schranke-Kriteriums der hypothetischen Datenneuerhebung in Anknüpfung an das den Strafprozessrechtlern bestens vertraute Merkmal des hypothetischen Ersatzeingriffs der Anwendungspraxis wesentliche Orientierungshilfen mit Strahlkraft auf die Gesamtmaterie geben können. Denn die Entscheidung darüber – das dürfen wir nie vergessen –, ob von einer nach den Grundsätzen der Zweckbindung und Zweckänderung noch erlaubten oder unerlaubten Datennutzung auszugehen ist, kann, so sehr er sich auch anstrengt, nicht dem Normanwender von dem Gesetzgeber abgenommen werden. Das wäre auch eine Verfehlung der Aufgabenteilung. Es ist nicht möglich, dem einzelnen Menschen, der in der Entscheidungssituation befangen ist, all das abzunehmen, sondern der Gesetzgeber muss, so hat das Bundesverfassungsgericht sehr schön mit dem Leitbild des Doppeltürmodells zum Ausdruck gebracht, dafür sorgen, dass die Doppeltüren geschmiert sind und rechtsstaatlichen Kriterien entsprechen. Nur das kann unsere Aufgabe sein und das wird mit dem Entwurf im Wesentlichen in hervorragender Weise erreicht. Danke.

Der **Vorsitzende**: Vielen Dank, Herr Gieg. Frau Halbritter, bitte.

SVe **Ria Halbritter**: Guten Tag! Auch ich freue mich, hier zu sein und bedanke mich. Ich bin Ria Halbritter, Rechtsanwältin, und komme für die Strafverteidigervereinigung in Berlin. Auch ich als Verteidigerin finde das Gesetz grundsätzlich gut und es ist zu begrüßen, dass die prekären Datenschutzgrundvorgaben der EU umgesetzt werden. Das ist natürlich nichts, was generell zu kritisieren wäre. Ich sehe auch die Ambivalenz, weil wir hier einen Sonderbereich haben, der auf das eigentliche Datenschutzrecht nicht zugeschnitten ist. Nämlich dass wir im Strafverfahrensrecht irgendwie die Ambivalenz zu klären haben, dass der staatliche Anspruch auf Ermittlung im Geheimen einerseits natürlich gewahrt werden muss und andererseits aber eben diese enormen Auskunftsrechte und datenschutzrechtlichen Rechte nun zu implementieren sind und von der EU vorgegeben werden. Das ist ein Spannungsverhältnis, das das Gesetz teilweise löst und aus meiner Sicht teilweise auch gut löst. Ich begrüße insbesondere, dass die aus der EU-Richtlinie vorgegebene Definition des Profilings und auch das Profilingverbot

übernommen worden sind. Ich erinnere daran, dass mit Art. 1 Abs. 3 der Richtlinie den Mitgliedstaaten aufgegeben bzw. erlaubt worden ist, auch strengere Regelung zu fassen und meine, dass man das als Ansporn nehmen sollte, hier den Datenschutz in Deutschland fortzuentwickeln und sich dabei möglicherweise auch als Speerspitze in der EU zu generieren. Zum Rechtlichen möchte ich auf drei Punkte zu sprechen kommen. Da greife ich die Kritik meiner Vorredner auf, dass die Frage des Konkurrenzverhältnisses zur Anwendung einerseits des BDSG, andererseits vielleicht noch der Richtlinie und dann eben der Regelung in der StPO zu kompliziert und für den Anwender nicht wirklich anwenderfreundlich ist, und man insoweit letztendlich keine gute Rechtsfindung und Rechtsanwendung erwarten darf, wenn man hierzu schon die Gesetzesbegründung mehrmals lesen muss, um verstehen zu können, wie das gemeint ist. Wenn ich es richtig verstanden habe, dann wird hier gesagt, dass beispielsweise die allgemeinen Regelungen des BDSG vorherrschen sollen und nur in einem zweiten Schritt geschaut werden soll, ob die Sonderreglungen, die bereichsspezifischen Regelungen der StPO, gelten sollen. Das ist juristisch ungewöhnlich. Normalerweise wird das meiner Kenntnis nach umgekehrt gestaltet und ich meine, dass man den Gesetzgeber hier auffordern sollte, eine bessere Struktur und eine bessere Verweisungstechnik einzubauen. Ich sehe auch eine fehlende Stringenz zwischen den eigentlichen Regelungen in der StPO einerseits, die beispielsweise Akteneinsichtsrechte für Verletzte und Nebenkläger erlauben, und andererseits den Regelungen über Auskunftsansprüche und Informationsrechte von Dritten oder vielleicht noch Zeugen, die also gar nichts mehr mit dem Strafprozess an sich zu tun haben. Dass diese Auskunftsrechte so sehr gestärkt werden, ist grundsätzlich schön, aber umgekehrt wird nicht bedacht, dass das natürlich die Rechte der eigentlichen Subjekte im Strafverfahren, nämlich die der Beschuldigten, massiv einschränkt, wenn die Möglichkeiten für Dritte, Einsicht in Akten und Informationen usw. zu bekommen, immer mehr ausgeweitet werden. Ich kritisiere auch das Modell der Löschungspflicht. § 58 Abs. 3 Nr. 3 BDSG soll gelten, in dem unter anderem geregelt ist, dass keine Löschung vorzunehmen ist, wenn sie einen unverhältnismäßigen Aufwand bedeuten würde. Das ist zu kritisieren, zumal der § 58 Abs. 3 Satz 3 BDSG sich in Art. 16 der Richtlinie – meine ich – nicht findet und insofern von der Richtlinie nicht vorgegeben worden ist. Letztendlich ist es so, dass in der Praxis – das kann ich Ihnen versichern – all das überhaupt keine Rolle spielt und überhaupt keine Sensibilisierung der Beteiligten zu bemerken ist. Sie werden auch beispielsweise einiges googeln müssen und die Informationen über den Datenschutz nicht ohne Weiteres auf der Seite des Landgerichts Berlin beispielsweise finden. Das ist alles nicht anwenderfreundlich.

Der **Vorsitzende**: Vielen Dank, Frau Halbritter. Herr Kegel bitte.

SV **Matthias Kegel**: Sehr geehrte Abgeordnete, sehr geehrte Damen und Herren! Bevor ich auf drei Aspekte zum vorliegenden Gesetzentwurf eingehe, möchte ich mich ganz kurz vorstellen: Ich bin bei der Generalstaatsanwaltschaft des Landes Brandenburg IT-Dezernent und bin einer der Väter des staatsanwaltschaftlichen Fachverfahrens MESTA. Und naturgemäß beschäftigt man sich daher auch dort mit dem Datenschutz, insbesondere mit den Regelungen §§ 483 ff., § 489 StPO und den Regelungen nunmehr aus dem BDSG Teil 3.

Zunächst möchte ich etwas ausführen zur Erhebung retrograder Daten mit der Neuregelung in § 100g Abs. 1 Satz 2 und 3 StPO-E. Ich möchte folgende Fragen beantworten: Senkt die Regelung das Datenschutzniveau? Widerspricht sie der Intention des Gesetzgebers aus 2015? Und: Werden dadurch den Strafverfolgungsbehörden mehr Befugnisse eingeräumt? Ein kurzer Blick in die Gesetzesgeschichte: Als am 18. Dezember 2015 die Neufassung von § 100g Abs. 2 StPO in Kraft trat, gab es eine kurzzeitige, bewusste Vollzugslücke beim Abruf der Standortdaten aus den nach § 113b Telekommunikationsgesetz (TKG) zu speichernden Vorratsdaten. Denn der Gesetzgeber räumte den Providern anderthalb Jahre Zeit ein für die technische Umsetzung der

Speicherung der Vorratsdaten. Da somit in dieser Zeit ein Abruf der Standortdaten aus dem Vorratsdatenpool nicht möglich war, wäre Abs. 2 ins Leere gelaufen. Der gesetzgeberische Wille war jedoch ein lückenloser retrograder Abruf von Standortdaten. Diese Vollzugslücke schloss er mit einer Übergangsregelung im Einführungsgesetz zur StPO und erlaubte einen Zugriff auf die nach § 96 TKG gespeicherten Standortdaten. Faktisch bestand auch nach dem 1. Juli – nach Ablauf der Frist – für die Provider das Vollzugshemmnis fort. Denn fast alle Provider speichern nach einer Erklärung der Bundesnetzagentur überhaupt keine Vorratsdaten mehr. Damit wird die Aufklärung von schweren Straftaten erschwert, wenn nicht gar verhindert. Nunmehr soll durch die neue Regelung die nach wie vor bestehende gleiche Vollzugslücke – ähnlich wie 2015 – geschlossen werden und der Zugriff auf die von den Providern aus betrieblichen Gründen gespeicherten retrograden Standortdaten nach § 96 TKG zugelassen und zwar – das ist wichtig – in den engen gesetzlichen Grenzen aus Abs. 2. Daher ist die Regelung unbedenklich, sie widerspricht weder der Intention des Gesetzgebers aus 2015, noch werden damit die Befugnisse der Strafverfolgungsbehörden erweitert. Vielmehr wird dadurch eine nicht vorhersehbare planwidrige Vollzugslücke geschlossen. Zweiter Punkt meiner Ausführungen betrifft die Auskunftserteilung an betroffene Personen nach § 491 StPO-E. Das Bundesministerium der Justiz und für Verbraucherschutz hat in der Abstimmung zu dem Referentenentwurf die Einwände aus der staatsanwaltschaftlichen Praxis in § 491 Abs. 2 Satz 2 des Entwurfes aufgegriffen, um nämlich der Gefahr einer Ausforschung des staatsanwaltschaftlichen Fachverfahrens zu begegnen, so wie es zunächst der Referentenentwurf ermöglicht hätte. Danach kann nämlich jetzt der Bescheid – ähnlich wie bei der gegenwärtigen Regelung – eine Formulierung enthalten, aus der kein Rückschluss möglich ist, ob noch geheim zu haltende Ermittlungsverfahren vorliegen oder nicht, so dass der Ermittlungserfolg dieser Verfahren nicht gefährdet wird. Und noch abschließend zu § 500 StPO-E: Dass das BDSG für das gesamte Verfahren gelten soll, wird ausdrücklich begrüßt. Damit wird nämlich ein bundeseinheitlicher Datenschutzstandard bei Gerichten, Strafverfolgungsbehörden, Vollstreckungsbehörden, Bewährungshilfe usw. gewährleistet, eine länderspezifische Zersplitterung vermieden, und alle betroffenen Personen im Strafverfahren werden datenschutzrechtlich gleich behandelt. Anderenfalls käme es zu schwierigen länderspezifischen Anpassungsprogrammierungen in dem Fachverfahren. Recht schönen Dank.

Der **Vorsitzende**: Das war zeitlich gesehen eine Punktlandung – wunderbar. Der Nächste ist Herr Kelber. Bitte schön.

SV **Ulrich Kelber**: Sehr geehrter Herr Vorsitzender, meine Damen und Herren Abgeordnete, vielen Dank für die Möglichkeit, zu dem Gesetzentwurf auch mündlich Stellung nehmen zu können. Entschuldigen Sie noch einmal, dass ich in zeitlicher Hinsicht ein wenig beschränkt bin. Ich werde um 16.30 Uhr dann den Ausschusssaal wechseln müssen, weil der Ausschuss für Digitale Agenda zum US-Privacy-Shield-Abkommen Fragen hat. Ziel des vorliegenden Entwurfes sollte es vor allem sein, die JI-Richtlinie umzusetzen. Das erfolgt weitgehend durch redaktionelle Änderungen – aus Datenschutzsicht allerdings nicht ambitioniert genug und auch nicht vollständig. Aus dem Grundsatzurteil des Bundesverfassungsgerichts wird nur eine der Grundaussagen übernommen, zur hypothetischen Datenneuerhebung. Außerdem kommt eine wichtige Regelung hinein, die mit dem Urteil und auch der JI-Richtlinie nichts zu tun hat. Es geht nämlich um die Frage der Neuregelung zu den Strafverfahrensdateien. Damit würde ich auch gerne beginnen. Diese Regelung ist aus unserer Sicht misslungen. Sie führt zu einer erheblichen Absenkung des Datenschutzniveaus und in die bisherige Regelsystematik wird entsprechend eingegriffen. Es geht vor allem um die neue Möglichkeit, die Strafverfahrensdateien, die ja eigentlich Spezialdateien für ein einzelnes bestimmtes Strafverfahren sind, in die Informationssysteme der Polizeibehörden zu integrieren. Hier wächst zusammen, was nicht

zusammen gehört. Die Datenverarbeitung geschieht auf mehreren Ebenen, insbesondere am Anfang der polizeilichen und staatsanwaltschaftlichen Aufgabe. Hier können praktisch unbegrenzt Daten für das jeweilige Verfahren erhoben werden, also sehr große Spurensammlungen, digitalisierte Akten, Text-, Video-, Bild-, sonstige Daten, Daten aus Rasterfahndung und Funkzellenabfragen. Inhaltliche Grenzen setzt der Gesetzeswortlaut nicht. Im Gegenzug ist die Strafverfahrensdatei aber auf das jeweilige Strafverfahren und die damit befassten Ermittlerinnen und Ermittler begrenzt. Informationssysteme der Polizeibehörden dagegen sind etwas, wo viele Daten auf Vorrat für viele einsehbar sind, pauschal genutzt werden können. Welche Daten das sein dürfen und welche Personen erfasst werden dürfen, regelt etwa das Bundeskriminalamtsgesetz (BKA-Gesetz). Die gesetzlichen Schwellen darf eine Neuregelung nicht unterlaufen. Die neue Regelung grenzt aber nicht ein, mit welchem Datenkranz und mit welchen Zugriffsrechten die Strafverfahrensdateien in die Informationssysteme integriert werden sollen. Also welche Vorgaben sollen dafür gelten? Es gelten dann die StPO, das BKA-Gesetz und 16 Landespolizeigesetze nebeneinander. Wir glauben, dass die Regelung hier datenschutzrechtlich und rechtssystematisch problematisch ist. Zur Umsetzung der Richtlinien des Urteils selbst: Ich hatte gesagt „aus Datenschutzsicht nicht ambitioniert genug“, vielleicht an Beispielen: Es ging vor allem in dem Grundsatzurteil des Bundesverfassungsgerichts um die besonders eingriffsintensiven Ermittlungseingriffe, also zum Beispiel durch V-Personen. Deren Einsatz kann nach dem Urteil zum BKA-Gesetz jedenfalls nicht mehr auf die Generalklauseln der StPO gestützt werden. Intensive Grundrechtseingriffe benötigen eine genau formulierte Rechtsgrundlage, sonst sind sie unzulässig. Die Regeln, nach denen Nachrichtendienste und Strafverfolgungsbehörden personenbezogene Daten übermitteln dürfen, hat das Bundesverfassungsgericht ebenfalls behandelt, auch schon im Urteil zur Antiterrordatei. Ich erneuere die Kritik, die meine Vorgängerin auch in der schriftlichen Stellungnahme geäußert hatte, und auch schon zum Bundesverfassungsschutzgesetz geäußert hat. Es geht insbesondere auch um die Rolle der Einwilligungen, die können aus unserer Sicht nicht ausreichende Rechtsgrundlagen im JI-Bereich sein. Den Punkt der Mitzieh-Klausel wird sicherlich der Kollege Petri gleich noch ansprechen. Hier kommen wir dazu, dass Daten, die dann in die Informationssysteme übergehen, immer wieder erneuert werden in ihrer Speicherfrist, also dass auch sensible Daten von Opfern und Zeugen über viele Jahre erhalten bleiben, ohne die Möglichkeit der Korrektur und der Löschung. Vielen Dank.

Der **Vorsitzende**: Vielen Dank, Herr Kelber. Der Nächste ist Herr Moldenhauer. Bitte schön.

SV **Dr. Gerwin Moldenhauer**: Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren, vielen Dank, dass ich hier sein darf. Gerwin Moldenhauer, Oberstaatsanwalt beim Bundesgerichtshof. Ich beschränke mich auf zwei Normen des Gesetzentwurfs, die für die staatsanwaltschaftliche Praxis ganz wesentlich sind, nämlich § 161 StPO und § 479 StPO in der Fassung des Gesetzentwurfs. Der Entwurf regelt in § 161 Abs. 3 und 4 StPO die Verwendung von Daten, die nach anderen Gesetzen erhoben wurden, und in § 479 StPO-E die Verwendung der sog. Zufallsfunde jeweils neu. Die Neuregelung wird im Wesentlichen dadurch erreicht, dass die Worte „zu Beweiszwecken“ in den geltenden Vorschriften, also § 161 und § 477 StPO, gestrichen werden. Im Ergebnis ist so jegliche Verwendung von Daten, die mit bestimmten eingriffsintensiven Mitteln erhoben wurden, nur zur Aufklärung von Straftaten möglich, für die eine solche eingriffsintensive Maßnahme auch nach der StPO jeweils angeordnet werden könnte, oder bei „vergleichbar bedeutenden Straftaten“. Erst einmal in formeller Hinsicht: Die Generalklausel für staatsanwaltschaftliche Ermittlungen, der § 161 StPO, soll durch den Gesetzentwurf in Abs. 3 und 4 Regelungen für die Verwendung von Daten erhalten, die aufgrund eines anderen Gesetzes – also nicht aufgrund strafprozessualer Maßnahmen – erhoben wurden. Anknüpfungspunkt für eine

solche Verwendung – sofern keine Katalogtat vorliegt – ist die „Aufklärung vergleichbar bedeutender Straftaten“. Die Formulierung trägt zunächst nicht zur Normklarheit bei. Es sei auf die Diskussion hinsichtlich des Begriffs der Straftat von erheblicher Bedeutung hingewiesen. Soviel hier in gebotener Kürze.

Dann zum materiellen Teil: Die Verwendung von Daten als Spurenansatz wird in der Praxis erheblich eingeschränkt werden. Das den Strafprozess prägende Legalitätsprinzip wird in vielen Fällen leerlaufen. Im Einzelnen: Die Umsetzung im Gesetzentwurf beruht auf der Entscheidung des Bundesverfassungsgerichts zum BKA-Gesetz. Danach ist fraglich, ob § 161 StPO der verfassungsrechtlich gebotenen Begrenzung der zweckändernden Datennutzung – bezogen auf polizeipräventive Daten – ausreichend Rechnung trägt. Rechtspraktisch wird durch die Neuregelung sehr wahrscheinlich insbesondere ein Teil der polizeipräventiven Zufallserkenntnisse der Strafverfolgung nicht zugänglich sein. Gravierender – und meines Erachtens in der Form nicht geboten – ist die Einführung des § 479 Abs. 2 StPO-E. Dieser verweist nun für sämtliche Daten, die aufgrund der StPO erhoben wurden, auf § 161 Abs. 3 und Abs. 4 StPO. Die Regelung setzt damit den strafprozessualen Zufallsfund den Maßnahmen aus anderen Gesetzen gleich und entzieht ihn, sofern er keine Katalogtat oder vergleichbar bedeutende Straftat betrifft, ebenfalls der Strafverfolgung. Das widerspricht tradierten strafprozessualen Grundsätzen, geht über die durch das Bundesverfassungsgericht und die DSGVO aufgestellten Anforderungen hinaus. Grundsätzlich können bei eingriffsintensiven Maßnahmen, wie beispielsweise der Telekommunikationsüberwachung, nicht Katalogtaten betreffende Zufallsfunde zwar nicht zu Beweiszwecken verwertet werden, sie können aber als Ermittlungsansatz in weiteren Verfahren verwertet werden. Dies ist durch das Bundesverfassungsgericht anerkannt. Etwas anderes gilt nur für die spezialgesetzlichen Regelungen der akustischen Wohnraumüberwachung oder der Onlinedurchsuchung, was natürlich im Hinblick auf die andere Eingriffstiefe einleuchtet. Es ist anerkannt, dass eine Verwendung der Erkenntnisse als Ermittlungsansatz zwar zu einer Wiederholung oder Vertiefung des Grundrechtseingriffs führt, weil die Daten im weiteren Umfang von Verfahrensbeteiligten zur Kenntnis genommen werden. Bei rechtswidrigen Maßnahmen wäre das verwertbar, bei rechtmäßigen nicht. Ich möchte mit einem Beispiel schließen: Der Generalbundesanwalt (GBA) führt ein Verfahren wegen § 129a Strafgesetzbuch – Mitgliedschaft in einer terroristischen Vereinigung – und hat gegen einen Nichttatbeteiligten Erkenntnisse wegen Volksverhetzung oder eines Kfz-Aufbruchs. Diese Erkenntnisse könnten nach der Neuregelung als Zufallsfund möglicherweise nicht verwertet werden. Vielen Dank.

Der **Vorsitzende**: Herr Moldenhauer, das war zeitlich auch bei Ihnen eine Punktlandung. Vielen Dank. Herr Petri ist der Nächste. Bitte schön.

SV **Prof. Dr. Thomas Petri**: Auch ich bedanke mich für die Gelegenheit zur mündlichen Stellungnahme und möchte auf drei Aspekte in den Regelungen zur StPO eingehen. Das erste ist, dass – und da knüpfe ich an das an, was Herr Kelber gesagt hat – dass die Umsetzung der JI-Richtlinie wenig ambitioniert erfolgt ist. Ich möchte das einmal an ein, zwei Beispielen festmachen, nämlich zunächst einmal an den Informationspflichten der Strafverfolgungsbehörden. Wenn ich als Zeuge oder als Anzeigenerstatter eine Aussage treffe, dann wird es so sein, dass ich nach der Justizdatenschutzrichtlinie eigentlich informiert werden sollte über die beabsichtigten Verarbeitungen. Man kann dazu Ausnahmen vorsehen, wenn das aus Sicht der Strafverfolgungsbehörden – sagen wir mal – sachgerecht ist, weil ansonsten die Straftatenaufklärung nicht gelingt oder aus Gründen des Opferschutzes oder Ähnliches. Aber im Grundsatz ist das Regel-Ausnahme-Prinzip so: Die JI-Richtlinie sagt, dass die Information die Regel und die Nichtinformation die Ausnahme ist. Wenn Sie in die StPO hineinschauen, dann werden Sie feststellen, dass dort das Regel-Ausnahme-System eigentlich gerade andersherum ist. Sie haben für bestimmte, besonders gelagerte

Situationen schon die Verpflichtung, die Betroffenen zu informieren, im Regelfall aber nicht. Und das wird auch nicht geändert. Und das ist meines Erachtens defizitär. Sie werden zwar als Zeuge – und das habe ich selbst als Betroffener, aber auch als Kontrollbehörde wiederholt feststellen müssen – belehrt über Ihre Betroffenenrechte, meistens relativ lieblos, aber darüber, was denn jetzt mit Ihren Informationen, die Sie geben, geschieht, werden Sie völlig im Unklaren gelassen. Die Juristen können damit umgehen, aber ein Durchschnittsbürger ist völlig überfordert damit, das einzuordnen. Diese Kenntnisse benötigt man aber, um die Betroffenenrechte sachgerecht ausüben zu können. Also wenn ich jetzt beispielsweise die Zeugenvernehmungen betrachte: Ich muss doch wissen, was mit meinen Daten geschehen soll, damit ich meine Rechte aus § 68 StPO geltend machen kann und mich darauf einstellen kann. Das wäre der erste wichtige Punkt. Der zweite Punkt ist, dass die JI-Datenschutzrichtlinie ausdrücklich sagt, dass die Verarbeitungsgrundlage nur eine gesetzliche Befugnis sein kann. Die Einwilligung ist ein Fremdkörper nach der JI-Datenschutzrichtlinie und zwar aus guten Gründen, denn die Einwilligung setzt als Wirksamkeitsvoraussetzung die Freiwilligkeit voraus. Wie wollen Sie denn in einem Strafverfahren gegenüber einer Strafverfolgungsbehörde freiwillig einwilligen? Das ist in atypischen Situationen denkbar, aber nicht im Regelfall. Deswegen sagt die JI-Datenschutzrichtlinie, dass eine Zustimmung der betroffenen Person eigentlich immer nur sozusagen als rechtsstaatliches Add-on funktioniert. Wir haben aber in der StPO rund 20 Vorschriften, die die Einwilligung so nebenbei als eigenständige Verarbeitungsgrundlage voraussetzen. Das sollte beseitigt werden. Bei dem § 161 Abs. 3 StPO-E und bei dem § 479 Abs. 2 StPO-E kann man das einfach dadurch erreichen, dass man diese Formulierung „ohne Einwilligung der von der Maßnahme betroffenen Person“ schlichtweg streicht. Ein letztes war die Mitzieh-Klausel. Die Mitzieh-Klausel ist bei Gefahrenabwehrregeln sinnvoll, aber bei Strafverfahren würde ich dafür plädieren, die Vorschrift ersatzlos zu streichen. Danke schön.

Der **Vorsitzende**: Danke, Herr Petri. Frau Sander schließt den Reigen. Bitte schön.

SVe **Dr. Lisa Kathrin Sander**: Vielen Dank, Herr Vorsitzender. Meine Damen und Herren, auch ich werde mich wunschgemäß recht kurz fassen und nur zu den Punkten Stellung nehmen, die aus Sicht der Staatsanwaltschaften vorrangig sind. Erstens betrifft dies bereits den Regelungsansatz des Gesetzesvorhabens an sich. Darin ist zur Umsetzung der sog. JI-Richtlinie – wie bereits gehört – anstelle der bisherigen bereichsspezifischen Sonderregelung in der StPO ein weitergehender Rückgriff auf das neugefasste BDSG vorgesehen. Gegen diesen systematischen Regelungsansatz, wonach unter weitgehendem Absehen von einer strafverfahrensspezifischen Sonderregelung ein grundsätzlicher Rückgriff auf das subsidiäre BDSG erfolgen soll, bestehen erhebliche praktische Bedenken. Denn infolgedessen sind Einschränkungen der Verständlichkeit und eine wesentliche Erschwerung der Rechtsanwendung zu besorgen. Hier kann ich mich insbesondere den Ausführungen von Frau Dr. Bunge und Frau Halbritter anschließen. Die Notwendigkeit einer so grundlegenden Abkehr von der bisherigen bewährten Regelungstechnik im Sinne einer kompakten Verfahrensordnung ist schon angesichts der damit einhergehenden Praktikabilitätseinbußen nicht zu erkennen und insbesondere nach den Vorgaben der JI-Richtlinie nicht zwingend. Aus Sicht nicht nur der staatsanwaltschaftlichen, sondern der gesamten strafrechtlichen Anwendungspraxis erscheint vielmehr eine Umsetzung der JI-Richtlinie innerhalb der StPO sinnvoll und sachgerecht. Damit ist sichergestellt, dass der Rechtsanwender die einschlägigen Regeln in einem möglichst geschlossenen Gesetzeswerk vorfindet und nicht auf eine Reihe unterschiedlicher Rechtsquellen zurückgreifen muss. Zugleich wäre dies auch unter systematischen Gesichtspunkten vorzugswürdig. Gerade in einem so eingriffsintensiven und sensiblen Bereich wie dem Strafverfahren stellen die Handhabbarkeit und

Stringenz einer Verfahrensordnung einen Wert an sich dar. Und zwar nicht etwa im Interesse einer möglichst komfortablen Rechtsanwendung, sondern primär wegen der erforderlichen materiellen Schlüssigkeit.

Ich komme zu meinem zweiten Punkt: Bedenken in der Sache und zugleich exemplarisch für die Auswirkungen des soeben dargestellten Regelungsansatzes begegnet insbesondere die vorgesehene Aufhebung der bisherigen Sonderregelung zum allgemeinen datenschutzrechtlichen Auskunftsanspruch in § 491 StPO. Dazu soll die bislang vorgesehene teilweise Ausschlussklausel zu datenschutzrechtlichen Auskunftsansprüchen dahingehend abgeändert werden, dass das allgemeine Auskunftsrecht des BDSG Anwendung finden und nicht mehr durch andere, in der StPO geregelte Auskunfts- oder Akteneinsichtsrechte verdrängt werden soll. Das geltende Regelungskonzept einschließlich der Sperrfrist für laufende Verfahren hat sich jedoch bewährt und trägt den Belangen und Geheimhaltungsbedürfnissen der Strafverfolgungsbehörden einerseits und den Interessen der Betroffenen andererseits differenziert und angemessen Rechnung. Es sollte daher in Übereinstimmung mit der Stellungnahme des Bundesrates beibehalten werden, denn die Verhinderung von Gefährdungen des Untersuchungszwecks des nichtöffentlichen Ermittlungsverfahrens erfordert eine kohärente und zugleich strafverfahrensspezifische Regelung in der StPO. Die geltende Rechtslage ist – in weitergehender Übereinstimmung mit der Auffassung des Bundesrates – auch mit der JI-Richtlinie vereinbar.

Drittens möchte ich in aller Kürze noch auf das vorgesehene Datenschutzregime eingehen. Angesprochen sind damit die Aufsichtskompetenzen der staatlichen Datenschutzbeauftragten, für die Landesjustiz insoweit der landesrechtlichen Aufsichtsstellen. Nähere Maßgaben zum Verhältnis des entsprechenden Beschwerderechts des Betroffenen zu den strafprozessualen Rechtsbehelfen und der fachaufsichtlichen Hierarchie der Staatsanwaltschaften sind dem Gesetzentwurf nicht zu entnehmen. Insoweit wären weitere Prüfungen im Fortgang des Gesetzgebungsverfahrens aus praktischer Sicht wünschenswert. Um es abschließend nochmals zu betonen: Die Belange der Anwendungspraxis finden in dem Gesetzentwurf bislang aus staatsanwaltschaftlicher Sicht nicht hinreichend Berücksichtigung. Da der Regelungsansatz nach den Vorgaben der JI-Richtlinie nicht zwingend ist und sich aus praktischer Sicht nicht empfiehlt, sollte er mit Blick auf Verständlichkeit und Kohärenz der StPO dringend überdacht werden. Mit der Ergänzung der DSGVO um die JI-Richtlinie sollte gerade den Besonderheiten der Strafjustiz Rechnung getragen werden können. Diesen Spielraum sollte der Gesetzgeber auch gesetzestechnisch nutzen. Vielen Dank.

Der **Vorsitzende**: Vielen Dank, Frau Sander. Vielen Dank an Sie alle, auch für die Einhaltung der Redezeit. Wir eröffnen nun die erste Fragerunde. Der Herr Müller fängt an, dann Herr Martens und anschließend Herr Fechner. Wir verfahren in der Reihenfolge.

Abg. **Axel Müller** (CDU/CSU): Vielen Dank, Herr Vorsitzender, und vielen Dank für die Ausführungen der Sachverständigen. Ich fange mal so an: Transparenz ist ja immer schön, aber manchmal ist es vielleicht nicht zu empfehlen, wenn man das, was hinter dem Ganzen steht, auch transparent machen will. Insbesondere dazu dienen ja oftmals strafrechtliche Ermittlungen. Und so komme ich noch einmal zurück auf den § 491 StPO in der dann geltenden neuen Fassung. Frau Dr. Sander, Sie haben ja sehr dezidierte Ausführungen gemacht. Jetzt habe ich eine Frage, die ich sowohl an Sie, als auch an die Frau Dr. Bunge richten möchte, zum § 491 StPO-E, der den Ermittlungsbehörden die Möglichkeit nimmt, zunächst einmal intransparent gegenüber dem Beschuldigten zu ermitteln – wichtig vor allen Dingen natürlich in Verfahren gegen die Organisierte Kriminalität und in Betäubungsmittel-Verfahren. Die Regelung wird insoweit wieder ein bisschen eingeschränkt, als dass es ja Möglichkeiten gibt – wie es ja auch geschildert wurde –, zu sagen: „Ja, da läuft etwas gegen Dich, aber mehr sagen wir nicht.“ Oder es wird ein

Aktenzeichen mitgeteilt, so ist das ja irgendwie zu verstehen. Nur sind Sie – das ist meine Frage – nicht auch der Meinung, dass das unter Umständen schon manchmal viel zu viel ist?

Der **Vorsitzende**: Danke, Herr Müller. Nun Herr Martens und danach dann Herr Fechner.

Abg. **Dr. Jürgen Martens** (FDP): Vielen Dank auch von Seiten der FDP-Fraktion an die Sachverständigen, dass Sie sich die Zeit genommen haben und dieses sehr umfangreiche Gesetzeswerk durchgesehen haben. Herr Petri, Sie sprachen es an: Die Einwilligung im Strafverfahren – sie könnte doch zu der, ich sage jetzt mal, irrigen Annahme führen, dass mit der Verweigerung einer Einwilligung eine Datenerhebung unterbliebe. Dem ist aber nicht so. Deswegen die Frage: Ist das Instrument der Einwilligung im Strafverfahren überhaupt ein taugliches Instrument?

Der **Vorsitzende**: Danke schön. Herr Fechner, bitte schön, und danach Herr von Notz.

Abg. **Dr. Johannes Fechner** (SPD): Vielen Dank. Ich hätte eine Frage an Herrn Dr. Moldenhauer. Sie sprachen davon, dass die Nutzbarkeit von Zufallsfunden als Ermittlungsansatz erheblich oder zu sehr eingeschränkt würde. Da würde mich zum einen interessieren, wie Sie das vor dem Hintergrund des Urteils des Bundesverfassungsgerichts zum BKA-Gesetz und vor dem Hintergrund der von Ihnen angesprochenen Entscheidung des Gerichts aus 2005 sehen. Wäre es aus Ihrer Sicht verfassungsrechtlich möglich, § 161 Abs. 3 StPO-E so zu ändern, dass die Zufallsfunde umfangreicher als bisher für die Staatsanwaltschaften als Ermittlungsansatz nutzbar sind? Und die zweite Frage wäre: Wie könnte eine so verfassungsgemäß ausgestaltete Regelung aussehen? Im Moment heißt es ja jeweils „vergleichbar bedeutende Straftaten“. Da wären ja bestimmte Straftaten dann nicht mehr dabei, die Sie nannten. Das wären meine beiden Fragen an Sie.

Der **Vorsitzende**: Nun Herr von Notz und danach Herr Straetmanns.

Abg. **Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Erstmal herzlichen Dank für die Stellungnahmen und Ihren Blickwinkel auf diese Reform. Ich frage mich vor allen Dingen bei der Norm des § 483 StPO-E, ob hier nicht ein sehr grundsätzlicher Paradigmenwechsel Einzug hält, wie das der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auch formuliert hat. Das würde sich dann ja im Grunde nahtlos anfügen an diese verunglückte Reform des BKA-Gesetzes, also in Bezug auf die Frage – gerade im digitalen Zeitalter, in dem wir uns befinden –, ob man hier nicht zu uferlosen Datenpools kommt? Also was bedeutet der § 483 des Entwurfs für die StPO? Welche konkreten Risiken sind damit verbunden, wenn alle nur erdenklichen Daten eines strafrechtlichen Ermittlungsverfahrens – und wenn ich es richtig verstehe, sowohl Opfer- wie auch Täterdaten – in einen großen polizeilichen Datenpool kommen? Ist das nicht der Dammbruch bezüglich unseres bisherigen Verständnisses zwischen repressiv polizeilichen und präventiv polizeilichen Datenhaltungen, die wir eigentlich hatten? Die Frage richtet sich an den Bundesdatenschutzbeauftragten und an Herrn Petri.

Der **Vorsitzende**: Danke schön. Und dann hatten wir noch Herrn Straetmanns, bitte schön.

Abg. **Friedrich Straetmanns** (DIE LINKE.): Ich hab eine Frage an die Frau Rechtsanwältin Halbritter. Und zwar haben wir ja zuletzt mit dem Urteil des Bundesverfassungsgerichts zum BKA-Gesetz ein Grundsatzurteil zur Verarbeitung von Daten aus heimlichen Ermittlungsmaßnahmen vorliegen. Und dazu gehören natürlich auch alle Erkenntnisse, die mit Hilfe von V-Leuten ermittelt worden sind. Greift aus Ihrer Sicht der Gesetzentwurf diese Problemstellung hinreichend auf? Oder welche Probleme sehen Sie, wenn die über V-Leute ermittelten Daten aus polizeilichen und nachrichtendienstlichen Zusammenhängen in das Strafverfahren eingeführt werden sollen? Vielen Dank.

Der **Vorsitzende**: Danke, Herr Straetmanns. Die

Rednerliste ist erschöpft für die erste Fragerunde. Dann schreiten wir zu den Antworten. Wir beginnen bei Frau Sander. Gestellt wurde eine Frage von Herrn Müller. Bitte schön.

SVe **Dr. Lisa Kathrin Sander**: Ja, Herr Müller, vielen Dank. Aus Sicht der Staatsanwaltschaft liegt die Problematik meines Erachtens nicht in der Negativauskunft, die zunächst neutral ist, sondern im Bereich der Auskunftsansprüche zeigt sich vielmehr das Erfordernis einer strafverfahrensspezifischen Regelung. Dabei ist zu berücksichtigen, dass Strafverfahren stets mehrpolig sind. Die entsprechende Abwägung der berechtigten Geheimhaltungserfordernisse der Staatsanwaltschaft mit Blick auf die Gefährdung des Untersuchungszwecks und der schutzwürdigen Belange Dritter – das mag der Beschuldigte sein, das können Geschädigte und weitere Verfahrensbeteiligte sein – mit Auskunftsinteressen, diese vermag das BDSG mit seinen allgemeinen Kriterien nicht vergleichbar abzubilden wie die StPO dies tut, in der diese Interessen bereits sorgsam austariert sind. In der ausdifferenzierten Systematik der Akteneinsichtsrechte sind nämlich die genannten Kriterien bereits in die gesetzgeberische Abwägung voreingestellt und eingeflossen und nicht lediglich Aspekte einer Einzelfallabwägung, wie nach dem BDSG. Man mag jetzt etwa an § 147 Abs. 2 StPO oder auch § 406e StPO denken. Bei den Akteneinsichtsrechten sind ganz explizit schutzwürdige Interessen Beschuldigter oder Dritter, die Gefährdung des Untersuchungszwecks oder auch eine Verzögerung des Verfahrens benannt. Ich kann daher nur nochmals sehr dringend für die Beibehaltung dieses Systems plädieren. Vielen Dank.

Der **Vorsitzende**: Danke schön. Herr Petri, hat zwei Fragen gestellt bekommen – eine von Herrn Martens und eine von Herrn von Notz. Bitte.

SV **Prof. Dr. Thomas Petri**: Danke schön, Herr Vorsitzender. Ist das Instrument der Einwilligung generell untauglich? Das kommt drauf an, worauf es sich bezieht. Bezogen auf die typischen Fälle: Ja, da ist es untauglich, wenn neben der Einwilligung noch eine gesetzliche Verarbeitungsbefugnis besteht. Es gibt einzelne Regelungen in der StPO, da würde ich zögern, zum Beispiel beim Täter-Opfer-Ausgleich. Das ist eine atypische Situation. Da kann man natürlich auch sagen, dass man wirksam einwilligen kann, weil im Prinzip hier das zentrale Moment die Freiwilligkeit ist. Der Täter-Opfer-Ausgleich ist typischerweise freiwillig, von Freiwilligkeit geprägt, da funktioniert die Einwilligung. Aber da, wo eine Erhebungsbefugnis dahintersteht, da funktioniert es typischerweise nicht. Es gibt in der Richtlinie zwei Regelbeispiele: Das eine Regelbeispiel verstehe ich nicht so ganz, das sind die DNA-Erhebungen und die elektronische Aufenthaltsüberwachung. Bei der DNA-Datenerhebung ist das nicht so unproblematisch und leider ist das dort auch recht allgemein gehalten. Bei der elektronischen Aufenthaltsüberwachung würde ich dann schon eher wieder dazu tendieren zu sagen: „Naja, in Herrgotts Namen kann man eine Zustimmung als rechtsstaatliches Add-on zu einer Verarbeitungsgrundlage schon zulassen.“ Beim zweiten Beispiel geht es vor allem um eine Vollzugslockerung und die Frage einer Vollzugslockerung auf Basis einer zusätzlichen Zustimmung. Da würde ich das auch noch sehen können, dass man die Einwilligung belässt. Aber im Übrigen – weg damit! Das kann man relativ einfach streichen. Das hat nichts im Strafverfahren zu suchen. Der zweite Aspekt war der, wenn ich mich recht erinnere, von Herrn von Notz angesprochene Dammbruch. Also ich sage mal so: wenn Sie in dem § 483 StPO-E – genauso im Übrigen wie bei dem § 489 StPO-E bei der Mitzieh-Klausel, da haben wir auch diese Frage in etwas anderer Form –, abstellen auf Informationssysteme, dann ist das nicht nur das Informationssystem, was jetzt durch das BKA-Gesetz vorgesehen ist. Darüber müssen Sie sich im Klaren sein. Sondern das sind dann alle Informationssysteme, die in Sicherheitsgesetzen vorgesehen sind. Das ist ein Wechsel auf die Zukunft. Ich hab den Gesetzentwurf zum Anlass genommen, mal bei mir im bayerischen Polizeirecht darauf zu schauen. Da gibt es überhaupt nicht den Begriff des Informationssystems, zumindest nicht den polizeirechtlichen. Das ist kein geschützter Begriff. Und die Sachsen verstehen unter „Informationssystem“ etwas

anderes als der Bund und die Thüringer und die Niedersachsen verstehen noch einmal etwas anderes darunter. Darüber muss man sich im Klaren sein, wenn Sie den Begriff des Informationssystems einführen. Also wenn man da so etwas macht, dann wäre es dann auch sinnvoll zu definieren, was man darunter versteht. Ich würde davor warnen, darauf zu rekurrieren. Also insofern sehe ich den § 483 StPO-E auch als sehr problematisch an, weil dieser schon ein relativ weites Fass im Hinblick auf die Verwertbarkeit polizeilicher Daten im Strafverfahren aufmacht. Das ist nicht unproblematisch.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Herr Vorsitzender, darf ich ganz kurz nachfragen?

Der **Vorsitzende**: Ausnahmsweise.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Das ist nett, vielen Dank. Noch einmal zu der Frage „Welche Daten aus einem Strafverfahren?“ Nehmen wir an, es gibt einen Vergewaltigungsfall: Die DNA-Daten des Opfers – kommen diese in die Datenbanken? Kommen die Opferdaten in diese Datenbanken? Kommen die Daten der Zeugen in diese Datenbanken? Ich lese das so. Das ist doch verheerend, jetzt einmal im Ernst.

Der **Vorsitzende**: Herr Petri, wollen Sie hierzu etwas sagen?

SV **Prof. Dr. Thomas Petri**: Hinsichtlich der DNA-Daten würde ich jetzt zögern, das müssten wir noch einmal genauer untersuchen. Da hätte ich meine Zweifel, weil es da spezifische Regelungen gibt, die ja auch Löschungen nach Abschluss eines Verfahrens vorsehen. Aber in anderen Bereichen haben Sie recht. In die Datenbanken kommen auch die Daten der Zeugen, natürlich.

Der **Vorsitzende**: Danke schön. Herr Moldenhauer ist dann der Nächste mit zwei Antworten auf die Fragen von Herrn Fechner, bitte schön.

SV **Dr. Gerwin Moldenhauer**: Vielen Dank. Ich beziehe mich auf die Fragen von Herrn Fechner. Zunächst zum Bundesverfassungsgericht, der BKA-Gesetz-Entscheidung und den Zufallsfunden. Das Bundesverfassungsgericht hatte ja im Rahmen der Entscheidung zum BKA-Gesetz sich insoweit zu § 161 StPO geäußert, dass es sich um eine Zweckänderung der Daten handelt. Das heißt, die Daten waren präventiv polizeirechtlich erfasst und sollten dann repressiv im Strafverfahren verwendet werden. Da hat das Bundesverfassungsgericht Kritik geäußert. Der Gesetzentwurf gibt jetzt vor, dass sämtliche strafprozessualen Daten, bei denen es sich nicht um eine neue Zweckerhebung handelt, sondern die die ganze Zeit dem Zweck der Strafverfolgung unterliegen, noch einmal durch dieses Nadelöhr müssen. In einem anderen Zusammenhang hat das Bundesverfassungsgericht die Zufallsfunde sehr wohl für verwertbar gehalten. Das ist gängige Praxis. Das war im Zusammenhang mit einer Entscheidung zu Telekommunikationsüberwachungsmaßnahmen. Und wir kennen das im Strafrecht ja auch, dass selbst wenn wir jetzt eine rechtswidrige Erhebung hätten, nicht zwingend ein Verwertungsverbot die Folge wäre. Wir müssen da genau unterscheiden: Wir haben das vielleicht zunächst nur als Spurenansatz, also wir haben beispielsweise eine djihadistische Schmiererei – es ist nur die Sachbeschädigung – und wir können es als Spurenansatz nutzen, um möglicherweise zu durchsuchen, welche Schuhe hatte er an, welche Kleidung usw. Und dann finden wird den Sprengstoff, was wir sonst noch nicht konnten. Und die Beweismittel, die ich aufgrund des Spurenansatzes finde, also der Sprengstoff, der ist dann verwertbar. Aber nach der jetzigen Regelung könnte ich bei so einem Bagatelldelikt möglicherweise gar nicht mehr meinem Auftrag nach Legalität gerecht werden. Das finde ich bedenklich. Der zweite Senat des Bundesverfassungsgerichts hatte wie gesagt in der anderen Entscheidung mit den Daten zum Spurenansatz keine Probleme bei der Telekommunikationsüberwachung. Dann kurz zu der Frage, wie man das regelt. Das ist natürlich eine Herausforderung für den Gesetzgeber. Wir Strafjuristen lesen das so, dass es nur für den Strengbeweis gilt, nicht als Ermittlungsansatz. Man müsste es deutlich machen, gerade für den Rechtsanwender in der Praxis. Das sind ja auch Fragen, die sehr schnell entschieden werden müssen, also bei Gefahr im

Verzug usw. Es ist ja auch Teil der Entscheidung, die die Polizei nachts im Rahmen der Bereitschaft treffen muss. Ich hätte jetzt auch gar nicht solche Bedenken, den Spurenansatz als solchen oder den Ermittlungsansatz freizugeben und das reinzuschreiben. Damit das klar geregelt ist, damit man weiß, dafür darf ich es verwerten, dann muss ich halt etwas Neues finden, wenn ich dann durchsuche und ich finde nichts – ja, dann ist es tot. Dann kann ich ihn nicht anklagen wegen Sachbeschädigung und ansonsten geht es weiter mit den neu gefundenen Beweismitteln. Vielen Dank.

Der **Vorsitzende**: Danke schön. Herr Kelber, eine Frage von Herrn von Notz.

SV **Ulrich Kelber**: Die Regelung des § 483 StPO-E – wir halten das schon für eine hoch problematische Regelung. Man muss sich nur einmal anschauen: Wann darf ich eigentlich Daten speichern darf, was ist die Unterscheidung? Es geht hier um den konkreten Zweck, zu erfüllende Aufgaben, zum Beispiel ein konkretes Strafverfahren, Dokumentation oder eben vorbeugende Gefahrenabwehr. Und vor allem: § 483 StPO-E erlaubt eben eine sehr umfangreiche Beweis- und Hinweismaterialsammlung in einem konkreten Strafverfahren. Es gibt also die konkrete Aufgabenerfüllung und das ist die zentrale Vorschrift, die das regelt. Sie verzichtet auf näher bestimmte Grenzen. Sie erlaubt eine umfassende Speicherung, ohne den Inhalt, die Dauer und die Möglichkeiten der Auswertung näher zu benennen. Und da werden dann tatsächlich alle Verdächtigten und Beschuldigten, Zeugen, Opfer, Hinweisgeber und sonstige Personen erfasst. So eine breite Sammlung ist natürlich nur verhältnismäßig, wenn sie dann tatsächlich auf ein konkretes jeweiliges Verfahren beschränkt bleibt oder vereinzelte Daten in ein anderes Verfahren überführt werden können, aber auch dort zur Aufgabenerfüllung. Problematisch würde es jetzt hier, wenn diese Daten zu pauschal in die Gefahrenvorsorge übernommen werden könnten oder die Daten nicht mehr ausreichend voneinander getrennt wären. Der Gesetzentwurf erlaubt die Verankerung dieser Dateien in den Informationssystemen. Und wenn man das zusammenbringt mit den neuen technischen Entwicklungen, mit dem fast vollständigen Fehlen der Vorschriften, wie weiter verarbeitet werden kann, dann habe ich natürlich tatsächlich die Situation, dass sehr sensible Daten – selbst wenn es zu einzelnen noch Sonderregelungen gibt, wie Herr Petri es angedeutet hat – zusammengefasst werden, die an der Stelle nichts in den Dateien zur Gefahrenvorsorge zu suchen haben. Und natürlich spielt das zusammen mit der Mitzieh-Klausel, die wir aus Datenschutzgründen ohnehin schon für eine veraltete Regelung halten, die mit heutigen technischen Möglichkeiten ohnehin in eine neue Qualität umschlägt. Aber nehmen Sie den schlechtestmöglichen Fall, die Daten einer Hinweisgeberin oder eines Hinweisgebers kommen dann in das Informationssystem. Ein paar Jahre später sind Sie Zeuge und vielleicht noch einmal Opfer. Die Mitzieh-Klausel bedeutet dann, dass die hoch sensiblen Daten, die da aufgenommen wurden, dort über viele Jahre stehen bleiben, ohne dass sie sogar Beschuldigte oder Beschuldigter waren in einem Verfahren. Sie können noch nicht einmal ggf. nachweisen, dass die Daten falsch gespeichert sind, weil die dazugehörigen Akten eventuell längst vernichtet sind, aber der Datenhinweis wegen der Mitzieh-Klausel eventuell weit über ein Jahrzehnt erhalten bleibt. Da würden wir Sie als Gesetzgeber dringend bitten, diese Regelung im Entwurf zu überdenken und abzuändern.

Der **Vorsitzende**: Danke, Herr Kelber. Die Frau Halbritter hat eine Frage bekommen von Herrn Straetmanns.

SVe **Ria Halbritter**: Die Informationen, die von V-Personen in die originäre Strafakte gelangen, die sind schon hoch problematisch genug, weil man eben überhaupt keine Chance hat, sich dagegen zu verteidigen. Man erfährt nicht, wer derjenige ist, woher er die Kenntnis hat und beispielsweise kann man nicht aufklären, ob derjenige Geld dafür bekommen hat. Wenn sich solche Informationen jetzt noch aus anderen Verfahren und anderen Quellen ergeben, dann ist das noch weniger angreifbar und dann wird das

Problem mit Blick darauf, dass der Beschuldigte ja das Subjekt des Strafverfahrens sein soll, noch mehr verschärft.

Der **Vorsitzende**: Danke schön. Und abschließend die Frau Bunge mit einer Antwort auf eine Frage von Herrn Müller.

SVe **Dr. Viktoria Bunge**: Ich glaube, Frau Sander hat zu dieser Frage ja schon relativ viel gesagt. Dem kann ich mich natürlich nur voll umfänglich anschließen. Ich möchte aber auch noch einmal die Chance ergreifen, um dafür zu plädieren, dass man doch diese zahlreichen Bezugnahmen auf das BDSG auflöst und tatsächlich eigene Regelungen für die StPO schafft, weil es einfach die Möglichkeit bietet, die Besonderheiten des Strafverfahrens in der StPO zu verankern und sich nicht auf so allgemein gehaltene Regelungen, wie sie im BDSG enthalten sind, bezieht. Das ist natürlich auch Sinn und Zweck des BDSG, dass es auf zahlreiche Konstellationen und Situationen zugeschnitten ist, aber das gilt bei der StPO halt nicht. Da gibt es ganz andere Zielsetzungen und gerade die kann man durch bereichsspezifisches Recht umsetzen, und das finde ich, sollte man auch tun.

Der **Vorsitzende**: Danke, Frau Bunge. Damit haben wir die erste Antwortrunde abgeschlossen. Sind noch Fragen unbeantwortet geblieben? Das scheint nicht der Fall zu sein. Dann beginnen wir mit der zweiten Fragerunde. Da hat sich als Erster Herr Martens gemeldet und dann Frau Bayram.

Abg. **Dr. Jürgen Martens** (FDP): Vielen Dank, Herr Vorsitzender. Herr Kelber hat es eben schon angesprochen, meine Frage bezieht sich auf die Mitzieh-Klausel des § 489 Abs. 5 StPO-E. Diese Regelung besagt, dass die Löschung von Daten unterbleiben kann, bis für alle – ich betone „alle“ – Eintragungen die Löschungsvoraussetzungen vorliegen. Das heißt, dass also auch das unwichtigste Datum über Hinweisgeber so lange perpetuieren, sich in Akten weiter verpflanzen kann, auch in Polizeidatensystemen, bis für sämtliche Daten aus diesen Verfahren die Löschungsvoraussetzungen vorliegen. Jetzt meine Frage: Wer überwacht das? Sie haben es auch schon angesprochen, das dürfte außerhalb der Verhältnismäßigkeit liegen. Das ist mit den Grundsätzen von Datenerhebung, Datenspeicherung, Datenverarbeitung und Löschung nicht mehr zu vereinbaren, auch schon nach den allgemeinen Regelungen des BDSG, ich glaube aber auch, nach der Richtlinie. Dazu meine Frage: Sind diese Regelungen erstens verhältnismäßig, zweitens sind sie von der Richtlinie gedeckt und geboten? Die Frage richtet sich an die Praktiker, Frau Dr. Bunge, Herrn Dr. Gieg und Herrn Dr. Moldenhauer.

Der **Vorsitzende**: Sie haben jetzt zwei Fragen an jeweils drei Leute gestellt. Das ist ein bisschen viel, Herr Martens. Sie müssen schon ein bisschen eingrenzen.

Abg. **Dr. Jürgen Martens** (FDP): Das ist eine Frage.

Der **Vorsitzende**: Aber eine Frage an drei Sachverständige.

Abg. **Dr. Jürgen Martens** (FDP): Die Frage lautet: „Ist es verhältnismäßig und ist es von der Richtlinie geboten“?

Der **Vorsitzende**: Das sind zwei Fragen. Wem haben Sie die gestellt?

Abg. **Dr. Jürgen Martens** (FDP): Den zuletzt Genannten: Frau Dr. Bunge, Herrn Dr. Gieg und Herrn Dr. Moldenhauer.

Der **Vorsitzende**: Sie können eine Frage an zwei Sachverständige oder eine Doppelfrage an einen Sachverständigen richten. Sie können nicht eine Doppelfrage drei Sachverständigen stellen. Dann müssen Sie sich entscheiden.

Abg. **Dr. Jürgen Martens** (FDP): Ja, okay. Dann richte ich die Fragen an die Frau Dr. Bunge.

Der **Vorsitzende**: Gut, zwei Fragen wurden an Frau Bunge gerichtet. Die Nächste ist Frau Bayram, bitte schön.

Abg. **Canan Bayram** (BÜNDNIS 90/DIE GRÜNEN): Guter Versuch, Herr Kollege. Ich versuche es einmal mit einer Frage an die beiden Sachverständigen, die für den Datenschutz zuständig sind. Und zwar hat der Sachverständige Herr Dr. Moldenhauer in seiner Stellungnahme auf ein Ermittlungshindernis, auf eine

möglicherweise Beeinträchtigung des Legalitätsprinzips hingewiesen, dergestalt, dass die Neuregelung die Verwertung von strafprozessualen Zufallsfunden bzw. Zufallserkenntnissen verhindere. Insoweit drohe ein absolutes Beweisverwertungsverbot durch den Datenschutz. Meine Frage an Sie beide: Sehen Sie das auch so oder haben Sie keinerlei Befürchtungen in der Hinsicht?

Der **Vorsitzende**: Danke schön. Nun Herr Fechner, dann Herr Straetmanns.

Abg. **Dr. Johannes Fechner** (SPD): Ich hätte zum gleichen Komplex, zum § 161 Abs. 3 StPO-E eine Frage an Sie, Herr Kegel, als Praktiker. Teilen Sie die Bedenken, die Herr Dr. Moldenhauer angesprochen hat, dass die Zufallsfunde nicht angemessen genutzt werden könnten bei Geltung dieser Regelung?

Der **Vorsitzende**: Herr Straetmanns, bitte.

Abg. **Friedrich Straetmanns** (DIE LINKE.): Ich habe eine Frage an Herrn Kelber und an Professor Petri und diese zielt auf den § 479 StPO-E. Inwieweit sehen Sie diese Vorschrift als problematisch an im Hinblick auf die verfassungsrechtlich geforderte informationelle Trennung zwischen Geheimdienst und Polizei und zugleich auch im Hinblick auf den Bestimmtheitsgrundsatz?

Der **Vorsitzende**: Dann hatte sich der Herr Müller noch gemeldet. Bitte sehr.

Abg. **Axel Müller** (CDU/CSU): Vielen Dank, Herr Vorsitzender. Ich habe noch eine Frage an den Herrn Dr. Moldenhauer. Sie haben ja Ausführungen gemacht zu den Verwendungsbeschränkungen des § 479 Abs. 2 StPO-E, das gilt im Übrigen ja auch für § 161 Abs. 2 und 3 StPO-E. Mich würde interessieren, ob Sie der Meinung sind, dass das über die angesprochene Entscheidung des Bundesverfassungsgerichts zur Neuerhebung von Daten hinausgeht, ob das denn so notwendig ist oder ob man hier nicht auch auf diese Fassung des § 479 Abs. 2 in der jetzt vorliegenden Form verzichten und dennoch der Rechtsprechung Genüge tun könnte. Das gilt natürlich auch für § 161 Abs. 2 und 3 StPO-E mit den entsprechenden Einschränkungen.

Der **Vorsitzende**: Danke sehr. Weitere Wortmeldungen sehe ich nicht. Herrn Martens haben wir hier vorgemerkt für weitere Fragerunden. Wir beginnen wieder alphabetisch bei Frau Bunge mit zwei Antworten auf die beiden Fragen von Herrn Martens. Bitte schön.

SVe **Dr. Viktoria Bunge**: Könnten Sie die Fragen noch einmal ganz kurz zusammenfassen, damit ich sichergehen kann, dass ich Sie richtig verstanden habe?

Der **Vorsitzende**: Ich gebe das einmal weiter an Herrn Martens. Könnten Sie die Fragen noch einmal ganz kurz zusammenfassen?

Abg. **Dr. Jürgen Martens** (FDP): Stichwort: § 489 Abs. 5 StPO-E, die sogenannte Mitzieh-Klausel mit ihren zeitlich unbegrenzten Löschungsvorgaben. Ist das verhältnismäßig und wird das von der Richtlinie verlangt?

SVe **Dr. Viktoria Bunge**: Vielen Dank, dann hatte ich Sie richtig verstanden. Ohne dass ich mich jetzt dezidiert mit dieser Vorschrift auseinandergesetzt habe – weil das ja auch schon viele andere Kollegen in ihren Stellungnahmen gemacht hatten –, sehe ich das ein wenig problematisch. Weil die Richtlinie ja vorgibt, dass gewisse Löschungsfristen vorzuschreiben sind. Die Richtlinie gibt auch vor, dass durch technische und organisatorische Maßnahmen sichergestellt werden muss, dass diese Löschungsfristen eingehalten werden. Hier sehe ich – wie gesagt, auf den ersten Blick – wenige solche organisatorischen oder technischen Maßnahmen. Auch sehe ich nicht, dass insoweit bestimmte Höchstfristen bestehen, sodass ich das – eine Löschungsfrist ist ja auch immer eine Ausprägung des Verhältnismäßigkeitsgrundsatzes – durchaus als problematisch ansehen würde.

Der **Vorsitzende**: Danke, Frau Bunge. Nächster ist der Herr Kegel mit einer Antwort für Herrn Fechner. Bitte schön.

SV **Matthias Kegel**: Ich kann mich eigentlich relativ kurz fassen: Die Kritik von Herrn

Dr. Moldenhauer unterstütze ich. Die Regelungen sind insoweit nicht ganz ausreichend und beschränken schon die Strafverfolgungsbehörden.

Der **Vorsitzende**: Danke sehr. Herr Kelber, wird noch beraten. Wir können Sie auch erst einmal überspringen?

SV **Ulrich Kelber**: Vielen Dank. Das ist tatsächlich für mich ein neuer Bereich im Vergleich zu dem, den ich früher hier im Ausschuss vertreten habe. Aber insbesondere zu § 479 StPO-E können Sie auch unserer schriftlichen Stellungnahme entnehmen, dass wir die Vorschrift in dieser Form für zu unbestimmt halten und insbesondere keine ausreichenden Schwellen an dem Punkt sehen. Wir glauben, dass das Bundesverfassungsgericht bezüglich der Übermittlungsvorschriften, die dieses informationelle Trennungsprinzip berühren, deutlich gemacht hat, dass es insoweit eine andere Regelung haben will, als nur eine, die für die Übermittlung auf die Notwendigkeit der Aufgabenerfüllung abstellt, dass es das in einer anderen Form begründet sehen wollte. Das ist unterblieben und gehört aus unserer Sicht zu den nicht ausreichenden Übertragungen. Der Punkt, der ja übernommen wurde aus dem Grundsatzurteil, betrifft die Fragestellung, wie Sie mit Daten umgehen, die Sie gewonnen haben durch den Einsatz schwerwiegender Eingriffe oder aufgrund von Zufallsfunden. Sie können diese nicht in einer anderen Form behandeln, nur weil sie über einen bestimmten Weg gefunden wurden, sondern Sie müssen die gleiche Rechtsgrundlage dafür besitzen, um sie theoretisch auch neu erheben zu können. Dieser Punkt ist aus unserer Sicht nicht anders übernehmbar aus dem Grundsatzurteil, als es hier geschehen ist.

Der **Vorsitzende**: Danke, Herr Kelber. Dann haben wir Herrn Moldenhauer mit einer Frage von Herrn Müller. Bitte.

SV **Dr. Gerwin Moldenhauer**: Vielen Dank, Herr Müller. Ich komme noch einmal zurück auf die Entscheidung zum BKA-Gesetz und das, was Herr Kelber gerade gesagt hat. Das Verfassungsgericht hat sich ja dort im Zusammenhang mit der Zweckbindung mit dem Problem befasst. Dieses Problem stellt sich im Strafverfahren grundsätzlich erst einmal nicht, wenn ich den Zweck so definiere, dass dieser „Strafverfolgung“ ist. Wenn ich den Zweck so definiere, Herr Kelber, dass ich einmal sage, Zweck sei die Aufklärung einer terroristischen Straftat und Zweck sei die Aufklärung eines Betruges, dann würde sich dieses Problem stellen. Das stellt sich aber meines Erachtens nicht. Und jetzt spreche ich als Praktiker und aus der forensischen Praxis: Gerade in Strafverfahren werden häufig – das Al-Capone-Prinzip kennen wir alle – durch solche Zufallsfunde Straftaten aufgeklärt. Man braucht also etwas Glück als Ermittler. Und uns das wegzunehmen, aus der Hand zu schlagen, ist aus meiner Sicht im Hinblick auf die Verfassungsrechtsprechung überobligatorisch. Und der Gesetzgeber hat es ja im anderen Zusammenhang so geregelt. Wir haben ja die Norm bei der Onlinedurchsuchung, bei der Wohnraumüberwachung. Da hat ja der Gesetzgeber gesagt „Bei so schweren Eingriffen dürft ihr nicht verwerten.“ Aber dass wir das jetzt bei sämtlichen Normen machen wollen, das geht über die Anforderungen – sowohl des Bundesverfassungsgerichts als auch der Datenschutz-Grundverordnung – hinaus. Deswegen würde ich das so nicht machen. Vielen Dank.

Der **Vorsitzende**: Danke Herr Moldenhauer. Herr Petri mit zwei Antworten, Frau Bayram und Herrn Straetmanns haben Fragen gestellt.

SV **Prof. Dr. Thomas Petri:** Zunächst einmal ist der Gesetzgeber nie gehindert, auch unbestimmte Rechtsbegriffe zu verwenden. Das ist klar. Soweit sich über Auslegungsmethoden der Sinn der Regelung erschließen lässt, wäre das jetzt per se nicht verfassungsrechtlich bedenklich. Wenn man jetzt einmal den Bereich der Strafverfolgung verlässt und in andere Bereiche hineingeht, also wenn Sie jetzt abheben auf die Übermittlung an Nachrichtendienste beispielsweise, da berührt eine etwaige Regelung das Prinzip der informationellen Trennung. Da gibt es das Urteil des Bundesverfassungsgerichts zum Antiterrordateigesetz, was gesagt hat, dass das nur unter besonderen Verhältnismäßigkeitsgrundsätzen zulässig ist. Man kann also diese informationelle Trennung aufheben, allerdings nur dann, wenn es

besondere Gründe dafür gibt, pauschal kann man es nicht.

Die zweite Frage war, glaube ich, die nach dem Verhältnis § 479 StPO-E zu § 161 StPO-E, wenn ich Sie richtig verstanden habe, Frau Bayram. Ich glaube, dass der Herr Moldenhauer da der Sache nach recht hat. Ich glaube aber auch, dass das der Sinn der Regelung ist, diese Begrenzung vorzunehmen. Also dass man sagt „Wir wollen bestimmte Verwendungsverbote einführen.“, das ist Sinn dieser Regelung. Dafür hat man sie so geändert, wie sie geändert worden ist. Also, man kann das natürlich aus Sicht der Strafverfolgungsbehörden kritisieren, das kann ich als Datenschützer schwer beurteilen, inwieweit das jetzt zu irreparablen Schäden in der Strafverfolgung führt. Das kann ich nicht seriös beurteilen. Aber, dass das der Umsetzung von Verwendungsbeschränkungsregelungen von Verfassungs wegen dient, das ist gewollt. Das steht ja auch ausdrücklich in der Gesetzesbegründung, dafür ist diese Regelung gemacht. Ich weiß nicht, ob das jetzt befriedigend für Sie ist, aber ich muss Ihnen sagen, dazu war ich zu wenig als Strafverfolger tätig, als Richter schon, aber als Strafverfolger noch nicht.

Der **Vorsitzende**: Nach unseren Unterlagen sind die Fragen abgearbeitet. Oder sind noch Fragen unbeantwortet geblieben in der zweiten Fragerunde? Das sehe ich nicht. Dann teile ich mit: Herr Kelber hat sich aus- und Herrn Bergemann eingewechselt. Herzlichen willkommen in der Runde. Ich glaube, es gibt insoweit keinen Widerspruch. Dann beginnen wir mit der dritten Fragerunde. Herr Martens, wollen Sie weitermachen?

Abg. **Dr. Jürgen Martens** (FDP): Der § 489 StPO-E, der hat es mir angetan. Ich stelle jetzt noch einmal die Frage an Herrn Professor Petri und Herrn Dr. Moldenhauer: Ist § 489 Abs. 5 StPO in der jetzt vorgeschlagenen Form verhältnismäßig?

Der **Vorsitzende**: Gut, haben wir notiert. Dann haben wir Frau Bayram noch einmal, bitte schön.

Abg. **Canan Bayram** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank. Ich hätte eine Frage wieder an Herrn Petri und eigentlich hätte ich die auch Herrn Kelber gestellt. Aber ich verstehe das jetzt so, dass er nicht da ist, dass ich aber meine Frage an den Vertreter stellen kann.

Der **Vorsitzende**: Das ist genau richtig und ich verrate Ihnen mal ein halbes Geheimnis: Herr Kelber sagte mir gerade, dass Herr Bergemann im Zweifel sogar besser informiert sei als er selbst.

Abg. **Canan Bayram** (BÜNDNIS 90/DIE GRÜNEN): Na, dann freue ich mich auf die Beantwortung der Frage. Der Gesetzentwurf enthält in Art. 1 Nr. 6 lit. a, lit. bb eine mit der Umsetzung der Richtlinie nicht zusammenhängende Regelung betreffend die Erhebung retrograder, aus betrieblichen Gründen von Providern gespeicherter Standortdaten in § 100g Abs. 1 Satz 3 StPO-E. Das wurde sozusagen bei Gelegenheit mitgeregelt. Ich weiß, die Regelung war außer Kraft getreten, die Wiederherstellung wurde von der Justizministerkonferenz zwar gefordert, weil die Staatsanwaltschaften sonst umständlich die § 96 TKG-Daten beschlagnahmen müssten bzw. die Rechtsprechung die Erhebung der Daten weiter via zweifelhafter Auslegung zulässt. Der Sachverständige Kegel hat den Sachverhalt ja auch in seiner Stellungnahme beschrieben. Es stellt sich mir aber eine andere Frage, und zwar an die von mir benannten Sachverständigen: Wo liegen die Grenzen der Speicherung betrieblicher Daten, insbesondere Standortdaten durch die Provider bzw. wozu müssen Provider Standortdaten überhaupt länger als vielleicht eine Reklamationsfrist bzw. Anrechnungs-, Abrechnungsfrist oder Ähnliches speichern? Was dürfen Sie da wie lange speichern?

Der **Vorsitzende**: Danke schön. Herr Straetmanns.

Abg. **Friedrich Straetmanns** (DIE LINKE.): Vielleicht habe ich es im Entwurf nicht gefunden. Mir stellt sich eine ganz simple, praktische Frage. Wenn wir Informationen sammeln, dann haben wir die Polizeibehörden und wir haben die Gerichte. Jetzt wird meinetwegen beim Gericht ein Verfahren abgeschlossen, wodurch auch immer. Inwieweit ist sichergestellt, dass wenn zum Beispiel ein Freispruch erfolgt, dass nicht weiter Daten bei Polizeibehörden, die zur

Einleitung des Verfahrens geführt haben, noch weiter gespeichert werden?

Der **Vorsitzende**: Danke schön. Die Frage war an wen gerichtet, Herr Straetmanns? An Herrn Petri. Weitere Wortmeldungen sehe ich nicht. Dann beginnen wir mit den Antworten, und zwar bei Herrn Petri. Drei Fragen: von dem Kollegen Martens, der Kollegin Bayram und dem Kollegen Straetmanns. Bitte schön.

SV **Prof. Dr. Thomas Petri**: Bitte geben Sie mir eine Rückmeldung, wenn ich aus Ihrer Sicht die jeweilige Frage nicht richtig verstanden habe.

Die erste Frage bezog sich auf die Datenspeicherung retrograder Daten durch Telekommunikations-Anbieter. Das beurteilt sich, wenn ich das richtig einordne, nach dem Telekommunikationsrecht und dort sind relativ lange Fristen vorgesehen. Ganz, ganz grob gesagt, können die Anbieter so lange speichern, wie sie das zur Vertragsabwicklung benötigen. Früher gab es ja eine 91-Tage-Frist, aber das ist durch die modernen Verträge hinfällig geworden. Also, im Prinzip gibt es tatsächlich Speicherungen, die sehr, sehr lange dauern, insbesondere wenn man Verträge hat, die über einen Anbieter hinausgehen. Das betrifft etwa Roaming-Verträge, da gibt es mehrere Anbieter, die wechselseitig abrechnen müssen und dann können da schon sehr, sehr lange Zeiträume im Raum stehen. Das muss man jedenfalls im Einzelfall beurteilen. Aber das sind teilweise sehr, sehr lange Speicherfristen.

Die zweite Frage war: „Was ist, wenn jemand freigesprochen wird?“ Dann kommt es drauf an: Die Polizei darf nach der Rechtsprechung Daten zu Gefahrenabwehrzwecken auch weiterhin speichern, wenn ein gewisser Restverdacht besteht und das Risiko der Wiederholung der Straftat im Raum steht. Wenn diese beiden Voraussetzungen zusammenkommen, darf die Polizei auch bei einem Freispruch Daten in polizeilichen Datenbanken zur vorbeugenden Straftatenbekämpfung speichern. Die Polizei darf nicht speichern, wenn sich aus den Gründen des Freispruchs ergibt, dass die Person vom Gericht für unschuldig befunden wird, also diese berühmte erwiesene Unschuld. Früher hat man dies auch als OKS-Vermerke bei der Staatsanwaltschaft bezeichnet. Wenn offensichtlich keine Straftat vorliegt, weil der Straftatbestand gar nicht verwirklicht ist, bei den Einstellungen nach § 170 Abs. 2 StPO, wenn die Staatsanwaltschaften sagen, dass der Verdacht sich nicht erhärtet hat, dann muss – zumindest nach bayerischem Verständnis – die Polizei die Daten dann löschen. Dazu bringe ich sie auch in der Regel. Ich habe insoweit in der Regel eine Erfolgsquote von 30 bis 40 Prozent, was diese ganzen Verfahrenseinstellungsfragen anbelangt. Wenn ich da einen Brief schreibe und sage, „Hier ist wieder nach § 170 Abs. 2 StPO eingestellt worden.“, dann ist die Erfolgsquote relativ hoch. Das gilt aber nicht immer. Es gibt Situationen, in denen ein Restverdacht von Substanz bleibt und dann beharrt die Polizei auch – und das darf sie auch – darauf, weiter zu speichern. Das darf sie, von Verfassungs wegen. Hierzu gibt es zwei Kammerentscheidungen des Bundesverfassungsgerichts.

Eine Frage hatten wir noch zur Verhältnismäßigkeit des § 489 Abs. 5 StPO-E. Der Gesetzentwurf ist ja eine Verbesserung gegenüber dem geltenden Recht insoweit, als dass man jetzt anknüpfen will an den Status des Beschuldigten. Das ist schon einmal eine deutliche Verbesserung. Wo ein neues Fass aufgemacht wird, ist bei dem Zusatz „oder einem Informationssystem“. Und insoweit hätte ich tatsächlich Verhältnismäßigkeitsprobleme. Aber im Prinzip würde ich sagen, handelt es sich um eine datenschutzrechtliche Verbesserung. Aber noch einmal: Mit dem Zusatz „oder einem Informationssystem“, wo ich auch gar nicht nachvollziehen kann, wieso das hinein genommen wurde, weil man sich da auch teilweise abhängig macht von landesgesetzlichen Regelungen, die man noch gar nicht überschauen kann, weil noch gar nicht alle Polizeigesetze angepasst sind. Den Zusatz würde ich herausnehmen. Das wäre meine dringliche Empfehlung und dann würde ich denken, dass das unter Verhältnismäßigkeitsgesichtspunkten schon verfassungskonform wäre.

Der **Vorsitzende**: Danke sehr. Herr Moldenhauer hatte ebenfalls eine Frage von Herrn Martens gestellt bekommen.

SV **Dr. Gerwin Moldenhauer**: Ja, auch zum § 489 Abs. 5 StPO-E und der Verhältnismäßigkeit. Es ist ein Ermessen eingeräumt, das heißt, es kann trotzdem gelöscht werden. Aber wir kennen ja so ein Löschungsmoratorium auch beispielsweise vom Untersuchungsausschuss, dass man erst einmal bei bestimmten Sachverhalten wirklich alles von links und rechts ausleuchten muss, damit man es beurteilen kann. Und wenn ich anfange, das peu à peu zu löschen, dann ist die Einschätzung irgendwann irreversibel. Und aus diesen Gründen denke ich, dass es schon verhältnismäßig ist, bis zum Vorliegen der Löschungsvoraussetzungen für alle Eintragungen zu warten.

Der **Vorsitzende**: Danke schön. Und nun noch eine Antwort von Herrn Bergemann auf die Frage von Frau Bayram.

SV **Nils Bergemann** (für SV Ulrich Kelber): Vielen Dank. Die retrograde Beauskunftung von Standortdaten meint ja nicht die GPS-Daten des Gerätes, sondern – nur zur Klarstellung – die Cell-IDs, die gespeichert werden, also die Funkzellendaten. Die können die Anbieter aus betrieblichen Gründen speichern, zum Beispiel zur Störungsbeseitigung bis zu sieben Tage oder zu Abrechnungszwecken. Und für Abrechnungszwecke ist die Speicherung möglich bis sechs Monate nach Rechnungserstellung. Dafür muss es dann allerdings auch auf die Standortdaten für die Abrechnung ankommen. Das betrifft beispielsweise Fälle, in denen im Ausland telefoniert worden ist und ein Roamingtarif in irgendeiner Form in Anspruch genommen wird, sodass dieser Standort für die Rechnung entscheidend ist oder bei älteren Tarifen, die an einen bestimmten Standort des Betroffenen anknüpfen, wie beispielsweise früher diese Home-Zonen, wo man so eine Festnetznummer im Mobilfunknetz bekam. Das wären Tarife, bei denen eine längere Speicherung denkbar ist. Bitte haken Sie nach, wenn Sie insoweit noch ergänzende Fragen haben.

Der **Vorsitzende**: Danke schön. Damit scheinen aus unserer Sicht alle Fragen der dritten Runde beantwortet zu sein. Es gibt keinen Widerspruch. Dann beginnen wir mit der vierten Fragerunde. Herr Martens hat wieder den Aufschlag, wenn noch etwas offen sein sollte.

Abg. **Dr. Jürgen Martens** (FDP): Danke. Im Moment habe ich eine Frage an den Bundesdatenschutzbeauftragten nach dem praktischen Nutzen. Stichwort: Straftatenkatalog in § 100a StPO. § 161 Abs. 4 StPO-E spricht von „vergleichbar bedeutenden Straftaten“. Welchen praktischen Nutzen hätte die Öffnung des Kataloges von § 100a StPO für die Datenerhebung und wie ließe sich dann das Ganze von der Datenschutzaufsicht im Hinblick auf den Datenschutz wirkungsvoll kontrollieren?

Der **Vorsitzende**: Herr von Notz hatte sich noch gemeldet, bitte.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ich habe noch einmal eine eher – glaube ich – triviale Frage an Herrn Petri und Herrn Bergemann. Man kennt es ja von seinem eigenen iPhone und den Telefondatenbanken, die man da selbst hat: Wie hält man sie eigentlich auf dem neuesten Stand und wie pflegt man sie und wer korrigiert gegebenenfalls mal etwas? Am Ende sind es Datenmühlen, über die wir hier reden, gigantomanischen Ausmaßes. Wie ist die Kontrolle eigentlich in der Praxis gewährleistet? Wenn Sie einmal im Jahr oder einmal alle fünf Jahre dann vorbeikommen und sich so eine Datei anschauen, sagt man dann zu Ihnen: „Herr Petri, da ist die Datenbank, bitte korrigieren Sie, was Ihnen auffällt?“ Oder gibt es Leute, die dort jeden Tag bienenfleißig sitzen und korrigieren und abgleichen, beispielsweise prüfen, ob es sich vielleicht um eine Namensverwechslung handelt? Also, wie ist die Kontrolle praktisch gewährleistet bei diesen Dingen, die – das wissen wir seit dem G-8-Gipfel – ein solches Stigmatisierungsrisiko bergen?

Der **Vorsitzende**: Danke sehr. Nun noch Herr Müller, bitte.

Abg. **Axel Müller** (CDU/CSU): Ich habe eine Frage, aber an zwei Sachverständige, nämlich an die Frau Dr. Bunge und die Frau Dr. Sander. Sie haben ja beide in Ihren Ausführungen – aus meiner Sicht durchaus nachvollziehbar und zu Recht – kritisiert, dass die ganze StPO durch die

vielfachen Verweise auf das BDSG und die einzelnen Normen immer unübersichtlicher wird. Das heißt, unter Umständen muss der Ermittler erst zahlreiche andere Gesetzestexte zu Rate ziehen, um zu wissen, was er nun noch darf oder nicht mehr darf. Ihr Vorschlag war, dass man mehr in die StPO hineinnehmen solle, damit das übersichtlich ist. Jetzt eine Frage von mir verbunden mit einem eigenen Gedanken: Könnte man nicht die etwas weniger tragenden datenschutzrechtlichen Normen, die nicht entscheidend sind für die Aufrechterhaltung des Datenschutzes und die Umsetzung der DSGVO sowie der Entscheidung des Bundesverfassungsgerichts über die hypothetische Datenneuerhebung, dadurch überschaubarer machen, dass man sagt: „Wir ändern in entscheidenden Teilen die Richtlinien für das Straf- und Bußgeldverfahren (RiStBV) und geben da den Praktikern etwas an die Hand, mit dem sie dann auch arbeiten können.“?

Der **Vorsitzende**: Danke schön. Ich sehe jetzt keine weiteren Fragen mehr. Wir kommen damit zur vierten Antwortrunde. Frau Bunge beginnt, Sie hatten eine Frage von Herrn Müller gestellt bekommen, bitte.

SVe **Dr. Viktoria Bunge**: Ja, genau. Ich kann meinen Aufruf eigentlich nur wiederholen. Ich finde es immer noch besser, wenn man eine Volllösung schafft, damit die StPO in sich schlüssig ist. Ich habe natürlich teilweise auch Verständnis dafür, dass man diese nicht überfrachten möchte. Ich bin derzeit im Bereich des Justizvollzuges tätig und da haben wir jetzt zum Beispiel einen Musterentwurf für ein Justizvollzugsdaten-schutzgesetz erarbeitet, das auch die Richtlinie umsetzt. Und da haben wir bereichsspezifisches Recht geschaffen, das gerade diese ganzen Datenverarbeitungsvorgänge für den Justizvollzug inklusive der Auskunftsrechte, der Benachrichtigungsrechte usw. regelt. Für die Punkte, die Sie angesprochen haben, die unserer Ansicht nach jetzt nicht so sehr spezifisch den Justizvollzug betreffen – die Meldung an die Datenschutzbeauftragten zum Beispiel, die Aufgaben der Datenschutzbeauftragten oder die Stellung der Landesdatenschutzbeauftragten – haben wir auf das allgemeine Datenschutzrecht verwiesen. Das, finde ich, hat auch den Vorteil, dass das – was ich, wie gesagt, sehr befürworte – ein in sich geschlossenes System ist, man allerdings für die Aspekte, die zum Beispiel Aufsichtsbefugnisse betreffen oder die nichts Spezifisches haben, Verweisungen vorsieht, sodass man im Land dann – hier wäre es dann ja bundesweit – gleiche Regelungen hat. Aber gerade für die Anwender ist es einfach einfacher, wenn man nicht verschiedene Regelungen hat. Wie bereits erwähnt wird im BDSG ja teilweise auch auf verschiedene Abschnitte verwiesen und möglicherweise landet man dann auch wieder in der DSGVO. Ich glaube, dass es nicht ausreichend wäre, nur die RiStBV zu ändern, weil das auch diese wiederum überfrachten würde. Außerdem ist zu bedenken, dass die Gesetze ja auch für die Bürger verständlich und zugänglich sein müssen und die RiStBV ist jetzt ja auch nicht etwas, was jedem so geläufig ist. Auch aus diesem Grunde finde ich es einfach schöner, wenn man die spezifischen Regelungen auch im spezifischen Recht findet.

Der **Vorsitzende**: Danke sehr. Nun bitte Herr Bergemann in Vertretung für Herrn Kelber mit Antworten auf eine Frage von Herrn Martens und eine Frage von Herrn von Notz.

SV **Nils Bergemann** (für SV Ulrich Kelber): Herr Abgeordneter Martens, der Straftatenkatalog des § 100a StPO ist ein abschließender Katalog. Man kann sich vielleicht über dessen Reichsweite rechtspolitisch streiten, aber es ist eine Entscheidung des Gesetzgebers, die dieser so auch für sinnvoll gehalten hat. Und man kann dazu vor allen Dingen auch sagen, dass es sich um eine bestimmte Regelung handelt, weil es ganz klar ist, wegen welcher Straftaten die Maßnahme genutzt werden darf und bei welchen nicht. Wenn es jetzt um die weitere Verwendung der erhobenen Daten geht, bekommen wir natürlich mit einer Formulierung, die auf „vergleichbare Straftaten“ oder „vergleichbar bedeutende Straftaten“ abstellt, eine Unklarheit und ich kann schwer einschätzen, wie sich das in der Rechtspraxis dann auswirken wird. Auf jeden Fall trägt das nicht zur Klarheit bei.

Die vermeintlich triviale Frage des Herrn Abgeordneten von Notz ist nicht trivial. Die Datenschutzkontrolle ist sozusagen unser tägliches Geschäft. Dazu muss man wissen, dass es eine Vielzahl polizeilicher Dateien gibt, die dann auch den Bereich der Strafverfolgung betreffen. In diesen Dateien ist wiederum eine Vielzahl von Datensätzen zu einer Vielzahl von Personen – also wir reden über viele Millionen erfasste Personen – enthalten. Und bei dem Personalbestand, den wir als Bundesbeauftragter, aber den vor allen Dingen auch die Landesbeauftragten haben, sind natürlich nur Stichproben möglich. Das ist dann ein relativ geringer Anteil der Daten, die von uns kontrolliert werden, sodass wir in der Praxis bei Kontrollen darauf achten, vor allen Dingen strukturelle Fehler in den Dateien zu finden. Beispielsweise haben wir gemeinsam mit den Landesbeauftragten eine Kontrolle der „Falldatei Rauschgift“ vorgenommen und dabei festgestellt, dass strukturell in sehr vielen Fällen die Dokumentation der Negativprognose fehlte, sodass ein großer Teil der gespeicherten Daten datenschutzrechtlich nicht zulässig gespeichert war. In solchen Fällen kommen wir dann auch dazu, dass eine Vielzahl von Datensätzen gelöscht werden muss. Aber es ist natürlich eher selten, dass wir einzelne Datensätze durch Stichprobenkontrollen herausgreifen, die wir dann ähnlich gründlich prüfen, wie ein Verwaltungsgericht das machen würde, wenn der Betroffene klagen würde. Das ist dann natürlich in dem Umfang schlicht nicht leistbar. Es ist gerade in Fällen, wo es – die Frage kam vorhin schon auf – zu Freisprüchen kommt oder zu Einstellungen, natürlich ein enormer Prüfungsaufwand für uns, auch festzustellen, ob nun ein solcher Restverdacht noch vorliegt oder nicht. Weshalb die datenschutzrechtliche Kontrolle auch praktisch ihre Grenzen findet.

Der **Vorsitzende**: Danke schön. Herr Petri bitte noch einmal mit einer Antwort auf eine Frage von Herrn von Notz.

SV **Prof. Dr. Thomas Petri**: Genau, das ist dieselbe Frage, die Herr Bergemann gerade beantwortet hat. Zunächst einmal beantworte ich sie theoretisch. Nach Art. 5 der Richtlinie gibt es Speicherprüffristen. Das heißt, die Polizeien haben die Möglichkeit, statt fixen Löschfristen Speicherprüffristen vorzunehmen. Ein Teil der Lösung besteht in der Technik. Das heißt, die Polizei – und darauf achten wir bei Prüfungen auch – muss sich in dem Informationssystem der Technik bedienen, dass spätestens nach Ablauf dieser Speicherprüffrist eine Prüfaufforderung an den Sachbearbeiter erfolgt. Spätestens dann muss geprüft werden. Im Übrigen ist es so, dass eigentlich die Speicherung nicht weiter hinterfragt wird, es sei denn, es kommt ein Impuls von außen. Das ist das, was die Polizei normalerweise macht. Wir prüfen die Polizei, also vor allem das Landeskriminalamt mit den zentralen großen Dateien jedes Jahr. Und ich habe ehemalige Polizisten und Staatsanwälte bei mir in den Reihen, die wissen auch, wonach sie suchen und werden immer fündig. Aber wir suchen natürlich – ähnlich wie Herr Bergemann es angedeutet hat – auch nach strukturellen Mängeln. Und ich kann jetzt nicht eine Vollprüfung sämtlicher Datensätze, bei denen nach § 170 Abs. 2 StPO eingestellt worden ist, durchführen. Das ist nicht zu leisten. Sondern man sucht sich dann insoweit einen Verfahrenstypus mit Besonderheiten heraus, bei dem man davon ausgeht, dass das besonders fehlerträchtig ist.

Der **Vorsitzende**: Ich habe den Eindruck, Herr von Notz hat eine Nachfrage? Gerne, bitte.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank, Herr Vorsitzender. Den strukturellen Prüfungsansatz, den verstehe ich. Aber die Stichprobe, die muss ja geringer sein als im Promille-Bereich, selbst in Bayern. Also selbst wenn man kein bundesweites Informationssystem hat. Das kann ja noch nicht einmal die Nadel im Heuhaufen sein.

SV **Prof. Dr. Thomas Petri**: Wir haben, um da mal ein Beispiel zu nennen, den bayerischen Kriminalaktennachweis (KAN) mit circa 4 Millionen Datensätzen bei circa 4 Millionen Betroffenen. Wenn wir uns jetzt die Einstellungen nach § 170 StPO anschauen, dann gucken wir uns vielleicht 100 Datensätze an. Das ist noch nicht einmal im Promille-Bereich, wenn ich das richtig

sehe. Aber anders geht es nicht. Weswegen wir eben auf technische Lösungen drängen, die bei Einstellungen nach § 170 Abs. 2 StPO die Selbstprüfung durch die Polizei unterstützen, um das einmal vorsichtig auszudrücken. Wir können tatsächlich nur die Nadel im Heuhaufen suchen. Da haben Sie recht.

Der **Vorsitzende**: Ich habe den Eindruck, es handelt sich dabei nicht um einen Heuhaufen, sondern um einen vollen Heuschober.

SV **Prof. Dr. Thomas Petri**: Ja, aber wir finden trotzdem ein paar Nadeln. Kürzlich hatten wir eine Trefferquote von 25 Prozent. Wir haben 40 geprüft und zehn davon waren rechtswidrig gespeichert, völlig unstreitig.

Der **Vorsitzende**: Danke schön, Herr Petri. Frau Sander hatte von Herrn Müller noch eine Frage gestellt bekommen. Bitte.

SVe **Dr. Lisa Kathrin Sander**: Die angesprochene RiStBV empfiehlt sich für nähere Erläuterungen und Maßgaben. In Einzelfragen vermag sie meines Erachtens jedoch eine Umsetzung der JI-Richtlinie auf Gesetzesebene und hier in sich geschlossen in der StPO nicht zu ersetzen. Vielen Dank.

Der **Vorsitzende**: Damit ist auch diese Frage beantwortet und die vierte Antwortrunde an ihrem Ende angelangt. Wir könnten jetzt bei Bedarf in die fünfte Fragerunde starten. Gibt es noch offene Fragen? Das ist nicht der Fall. Dann bedanke ich mich herzlich bei den Fragestellern und noch viel herzlicher bei den Sachverständigen. Vielen Dank auch Herrn Bergemann für die Einwechslung. Ich wünsche Ihnen einen guten Heimweg und Ihnen noch einen schönen Tag. Vielen Dank.

Schluss der Sitzung: 16:39 Uhr

Stephan Brandner, MdB
Vorsitzender

Anlagen: Stellungnahmen der Sachverständigen

Dr. Viktoria Bunge Kiel, den 19.02.2019

Stellungnahme zum 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

Der hier vorliegende Gesetzentwurf der Bundesregierung dient der Umsetzung der Richtlinie (EU) 2016/680 sowie der Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679.

Angesichts der Kürze der Vorbereitungszeit kann sich die Stellungnahme nur auf einige Punkte beziehen und nicht den Gesetzentwurf in Gänze beleuchten. Schwerpunkte der Stellungnahme bilden die Änderungen in der StPO und dem StVollzG.

I. Allgemeines

Der Gesetzentwurf nimmt die sprachlichen Anpassungen, die durch die Richtlinie (EU) 2016/680 und die Verordnung (EU) 2016/679 erforderlich geworden sind, vor. So werden z. B. aus dem „Betroffenen“ die „betroffene Person“, aus „Datei“ „Dateisysteme“ und aus dem ursprünglichen Begriff der „Sperrung“ die „Einschränkung der Verarbeitung“. Mit diesen sprachlichen Änderungen sind jedoch keine inhaltlichen Veränderungen verbunden.

II. Änderungen in der StPO

1. Allgemeines

a) Umsetzung der Rechtsprechung des Bundesverfassungsgerichts

Positiv zu bewerten ist, dass im Rahmen des Gesetzentwurfes auch versucht worden ist, die Rechtsprechung des Bundesverfassungsgerichts vom 20. April 2016 (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) umzusetzen. So findet sich in § 161 StPO-E und § 479 StPO-E der Grundsatz der hypothetischen Datenneuerhebung überwiegend umgesetzt. Hinsichtlich des § 479 Abs. 2 StPO-E ist dies nicht vollständig gelungen. Zum einen sind die in § 161 Abs. 3 und 4 geltenden Grundsätze nicht auf Datenübermittlungen nach § 479 Abs. 2 Satz 2 anwendbar („darüber hinaus“). Zudem ist der pauschale Verweis in § 479 Abs. 2 Nr. 3 StPO-E auf § 18 Bundesverfassungsschutzgesetz zu allgemein gehalten und enthält nicht die erforderlichen Übermittlungsschwellen.

Dagegen hat die Rechtsprechung des Bundesverfassungsgerichts hinsichtlich des Schutzes des Kernbereichs privater Lebensgestaltung in zahlreichen Vorschriften Berücksichtigung gefunden, z. B in den § 100f Abs. 4 StPO-E und § 100h Abs. 4 StPO-E sowie § 110a Abs. 1 StPO-E durch den Verweis auf § 100d Abs. 1 und 2 StPO. Dies wird befürwortet.

b) Hinweis auf die Datenschutzgrundverordnung

Positiv zu bewerten ist die in § 81f Abs. 2 Satz 4 StPO-E und § 476 Abs. 8 StPO-E genannte Verweisung und der damit verbundene Hinweis auf die Anwendbarkeit der Verordnung (EU) 2016/679 (im Folgenden: DS-GVO) auf die nicht-automatisierte Verarbeitung personenbezogener Daten durch Personen, die als nichtöffentliche Stelle i. S. d. § 2 Abs. 4 Bundesdatenschutzgesetz (BDSG) anzusehen sind. Der Entwurf soll klarstellen, dass die Vorschriften der DS-GVO auch anzuwenden sind, wenn eine solche nicht-öffentliche Stelle personenbezogene Daten nicht in einem Dateisystem gespeichert hat oder speichern will. Insbesondere verdeutlicht dieser Hinweis auch noch einmal, dass es – obwohl es grundsätzlich im Groben um das Strafverfahren geht – auch die DSG-VO Anwendung finden kann und dass jeweils immer zu prüfen ist, welche datenschutzrechtlichen Grundlagen im Einzelnen gelten.

c) Verweisungen in das Bundesdatenschutzgesetz (BDSG)

Nach hiesiger Einschätzung sind die zahlreichen Verweise sowie die Regelung des § 500 StPO-E verbesserungsbedürftig. In zahlreichen Regelungen (wie beispielsweise § 161 Abs. 2 Satz 1 und Satz 2 StPO-E, § 475 Abs. 1 Satz 1 StPO-E, § 489 Abs. 6 StPO-E) wird auf die Normen des BDSG verwiesen. Dies ist sicherlich rechtlich zulässig, jedoch anders als im Anwendungsbereich der DS-GVO nicht zwingend, so dass entsprechende Regelungen – auch unter Berücksichtigung der Besonderheiten eines Strafverfahrens - in die StPO aufgenommen werden sollten. Dies erhöht die Anwenderfreundlichkeit und führt auch nicht zu divergierenden Entscheidungen. Denn wie es im Gesetzentwurf auf Seite 44 heißt „*Bei einer nur teilweisen Regelung oder im Falle des Schweigens eines bereichsspezifischen Gesetzes kommt es maßgeblich darauf an, ob die spezifischen Regelungen des jeweiligen Gesetzes für einen bestimmten Bereich insgesamt umfassend und damit abschließend die Datenverarbeitung regeln sollen. Wenn dies nicht der Fall ist, kann subsidiär auf die Vorschriften des BDSG zurückgegriffen werden. (…) Soweit die StPO eigene, nicht abschließende datenschutzrechtliche Vorschriften enthält, treten sie ergänzend neben die allgemeinen Regelungen des BDSG.“* Insofern steht zu befürchten, dass die Frage, ob die StPO in diesen Fällen abschließend ist, unterschiedlich beantwortet wird.

d) Verarbeitung besonderer Kategorien personenbezogener Daten

Artikel 10 der Richtlinie (EU) 2016/680 sieht vor, dass die Verarbeitung besonderer Kategorie personenbezogener Daten, zu denen z. B. die rassische oder ethnische Herkunft oder Gesundheitsdaten sowie biometrische Daten zur eindeutigen Identifizierung, nur erlaubt ist, wenn sie unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte

und Freiheiten der betroffenen Personen erfolgt. In § 48 BDSG werden diese Vorgaben umgesetzt. Jedoch wird lediglich in § 161 Abs. 2 StPO-E auf § 48 BDSG verwiesen. Die besonderen Kategorien personenbezogener Daten sind jedoch nicht nur im Rahmen des Ermittlungsverfahrens relevant, sondern auch für das Straf- und Vollstreckungsverfahren. In anderen Vorschriften z. B. für die Übermittlung (für die automatische Übermittlung in § 493 StPO-E) sollte ebenfalls ein entsprechender Verweis oder eine klarstellende Regelung aufgenommen werden.

2. Regelungen im Einzelnen

a) §§ 474-477 StPO-E

Die §§ 474-477 StPO-E sollten dahingehend erweitert werden, dass auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können und des Weiteren eine Übermittlung auf elektronischem Wege möglich ist.

Die genannten Vorschriften setzen momentan vom Wortlaut voraus, dass die betreffenden Daten in Akten gespeichert sind. Im Hinblick auf die Bedeutung der elektronischen Daten und der Ausweitung der e-Akte sollten auch elektronisch gespeicherte personenbezogene Daten übermittelt werden können und darüber hinaus eine Übermittlung auf elektronischem Wege möglich sein. Dies ist auch Zielsetzung des Gesetzgebers, wonach die Regelungen grundsätzlich technikneutral zur Anwendung kommen sollen, d.h. unabhängig davon, ob personenbezogene Daten elektronisch oder in Papierform verarbeitet werden. (S. 44 des Gesetzentwurfes)

b) § 478 StPO-E Form der Datenübermittlungen

§ 478 StPO-E sollte ebenfalls eine elektronische Übermittlung vorsehen.

c) § 479 Abs. 4 StPO-E Übermittlungsverbote und Verwendungsbeschränkungen

In § 479 Abs. 4 StPO-E findet sich folgende Regelung:
„Wenn in den Fällen der §§ 474 bis 476
1. der Angeklagte freigesprochen, die Eröffnung des Hauptverfahrens abgelehnt oder das Verfahren eingestellt
wurde oder
2. die Verurteilung nicht in ein Führungszeugnis für Behörden aufgenommen wird und seit der Rechtskraft der Entscheidung mehr als zwei Jahre verstrichen sind,

dürfen Auskünfte aus den Akten und Akteneinsicht an nichtöffentliche Stellen nur gewährt werden, wenn ein rechtliches Interesse an der Kenntnis der Information glaubhaft gemacht ist und der frühere Beschuldigte kein schutzwürdiges Interesse an der Versagung hat.“

Bei der in Bezug genommenen Vorschrift des § 474 StPO findet jedoch keine Übermittlung an eine nichtöffentliche Stelle statt; bei den in § 474 StPO genannten Stellen handelt es sich stets um öffentliche Stellen. Zudem soll diese Regelung nach der Gesetzesbegründung (S. 66 des Gesetzentwurfes) dem bisherigen Abs. 3 des § 477 StPO entsprechen. Nach der Kommentierung (Meyer-Goßner/Schmitt, StPO, 60. Auflage, 2017, § 477 Rn. 13) schränkt der Absatz jedoch eine Übermittlung nur nach § 475 StPO ein. Insofern ist der § 474 StPO aus § 479 Abs. 4 StPO-E zu streichen.

d) § 487 Abs. 1 Satz 3 StPO Übermittlung gespeicherter Daten

In § 487 Abs. 1 Satz 3 StPO ist bisher geregelt:

„Bewährungshelfer dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung, erforderlich sind.“

In der Praxis stellt sich das Problem, dass nach dem Gesetzeswortlaut eine Übermittlung nur möglich ist, wenn die Probanden noch unter Aufsicht gestellt sind. Daraus folgt, dass eine Übermittlung nach § 487 Abs. 1 Satz 3 StPO nicht möglich ist, wenn der Widerruf bereits erfolgt ist und insbesondere dann auch rechtskräftig feststeht, dass ein Interesse und ein Bedarf an den zu übermittelnden Daten besteht, weil der Proband wieder in den Justiz- oder Maßregelvollzug aufgenommen werden wird. Folglich muss gerade in diesen Fällen wieder mit einer Schweigepflichtsentbindung gearbeitet werden. Dies erscheint nicht praktikabel und entspricht auch nicht der Intention bei der damaligen Änderung des § 487 StPO (noch in Fassung des damaligen Referentenentwurfes):

„Mit der Ergänzung des § 487 StPO soll die Weitergabe personenbezogener Daten von der Bewährungshilfe an den Vollzug erleichtert werden. Bewährungshilfe und Vollzug sind in ihrer Arbeit sehr weitgehend auf identische Informationen angewiesen. Bei einer Weiterleitung der Daten von der Bewährungshilfe an den Vollzug kann eine doppelte Datenerhebung möglicherweise vermieden oder jedenfalls verringert werden. Auch der Vollzugsplan kann so schneller erstellt und

umgesetzt werden, wenn der Vollzug die hierfür erforderlichen Daten unmittelbar von der Bewährungshilfe erhält."

e) § 493 Abs. 3 Satz 3 und 4 StPO-E: Automatisiertes Verfahren für Datenübermittlungen

Der Entwurf sieht folgende Regelung vor:

„*Im Rahmen der Protokollierung nach § 76 des Bundesdatenschutzgesetzes hat sie ergänzend zu den dort in Absatz 2 aufgeführten Daten die abgerufenen Daten, die Kennung der abrufenden Stelle und das Aktenzeichen des Empfängers zu protokollieren. Die Protokolldaten sind nach sechs Monaten zu* löschen".

Die Frist von 6 Monaten weicht von der in § 488 Abs. 3 Satz 4 StPO-E ab, in dem die Frist zwölf Monate beträgt.

Die Protokollierung dient dem Schutz des Rechts auf informationelle Selbstbestimmung und ist eine den Grundrechtseingriff abmildernde Verfahrenssicherung. Unter engen Voraussetzungen dürfen die Protokolle nach § 76 Abs. 3 BDSG u.a. auch für Strafverfahren genutzt werden. Die entsprechende Zweckänderung wird in Artikel 25 Abs. 2 der Richtlinie (EU) 2016/680 zugelassen.

Nach der Entscheidung des EuGH in der Rechtssache C-553/07 (EuGH, Urteil vom 7. Mai 2009, C-553/07) sind Protokolldaten für einen Zeitraum aufzubewahren, der es den betroffenen Personen ermöglicht, die Rechtmäßigkeit der Verarbeitung nachzuvollziehen. Das Bundesverfassungsgericht hat in seiner Entscheidung zum Bundeskriminalamtgesetz (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09) ausgeführt, dass durch technische und organisatorische Maßnahmen sichergestellt werden muss, dass die Protokolldaten der oder dem Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält. Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle kommt ihrer regelmäßigen Durchführung besondere Bedeutung zu. Die Kontrollen sind in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 141).

Zudem ist hier zu berücksichtigen, dass mit der Übermittlung von personenbezogenen Daten ein weiter – teilweise sogar noch weitgehender - Grundrechtseingriff verbunden ist und daher eine erhöhte Datenschutzkontrolle durch die oder den Landesdatenschutzbeauftragte/n ermöglicht werden sollte. Insofern erscheint eine Frist von sechs Monaten nicht ausreichend und sollte an § 488 Abs. 3 Satz 4 StPO-E angeglichen werden.

III. Änderungen im StVollzG-E

1. Allgemeines

Positiv zu bewerten ist aus hiesiger Sicht, dass die Gesetzesänderungen, welche aufgrund der DS-GVO notwendig geworden sind, auch dazu genutzt worden sind, Anpassungen vorzunehmen, welche sich aufgrund der Föderalismusreform und dem daran anschließenden Wechsel in der Gesetzgebungskompetenz für den Strafvollzug ergeben haben. Der Anwendungsbereich des StVollzG ist auf Zivilgefangene und den gerichtlichen Rechtsschutz beschränkt. Dies ist durch sprachliche Änderungen klargestellt worden.

2. Regelungen im Einzelnen

a) Akteneinsichtsrecht für die Mitglieder der Delegation des Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe

Dem Gesetzentwurf fehlt eine Regelung für das Akteneinsichtsrecht für die Mitglieder der Delegation des Ausschusses zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (im Folgenden CPT) für Gefangenenpersonalakten und Gesundheitsakten.

Es handelt sich dabei um höchst sensible Daten. Da insbesondere auch Gesundheitsakten betroffen sind und daher eine besondere Kategorie personenbezogener Daten vorliegt, sollte dieses Recht nur gewährt werden, sofern dies für die Aufgabenerfüllung des Ausschusses unbedingt erforderlich ist.

Eine entsprechende Regelung wird – soweit es von hier aus beurteilt werden kann – in nahezu alle landesrechtliche Regelungen aufgenommen. Um den Bediensteten in den Justizvollzugsanstalten eine Handlungssicherheit und Klarheit zu geben, sollte eine solche Regelung auch im StVollzG für die Zivilgefangenen aufgenommen werden.

b) Gleichlauf mit anderen Regelungen der LStVollzG bzw. JVollzDSG

Darüber hinaus ist zu überlegen, ob nicht einige technische Erneuerungen zur Erhöhung der Sicherheit in den Anstalten und deren datenschutzrechtliche Absicherung ebenfalls in das StVollzG mitaufgenommen werden sollten. Dies gilt insbesondere vor dem Hintergrund, dass Zivilgefangene nicht durchgehend von Strafgefangenen getrennt untergebracht werden. Zu denken wäre z. B. an das Auslesen von Datenspeichern oder das Erfassen und ggf. den Abgleich von biometrischen Merkmalen.

c) Regelung für ein Akteneinsichtsrecht in die Gesundheitsakten

§ 185 StVollzG-E setzt die Entscheidung des Bundesverfassungsgerichts zum Akteneinsichtsrecht in die Gesundheitsakten vom 20. Dezember 2016 (2 BvR 1541/15)

nicht um. Danach haben die Gefangenen grundsätzlich einen Anspruch auf Auskunft aus ihren und Einsicht in ihre Gesundheitsakten.

Das Bundesverfassungsgericht hat festgestellt, dass bezogen auf den Zugang zu Krankenakten das Recht auf Selbstbestimmung und die personale Würde des Patienten (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) gebietet, jedem Patienten gegenüber seinem Arzt und Krankenhaus grundsätzlich einen Anspruch auf Einsicht in die ihn betreffenden Krankenunterlagen einzuräumen. Dieses Einsichtsrecht ist zwar von Verfassungs wegen nicht ohne Einschränkungen gewährleistet. Es hat seine Grundlage aber unmittelbar in dem grundrechtlich gewährleisteten Selbstbestimmungsrecht des Patienten und muss daher nur zurücktreten, wenn ihm entsprechend wichtige Belange entgegenstehen.

Bei der demnach notwendigen Abwägung kommt nach dem Bundesverfassungsgericht dem Informationsinteresse des Patienten grundsätzlich erhebliches Gewicht zu. Ärztliche Krankenunterlagen beträfen mit ihren Angaben über Anamnese, Diagnose und therapeutische Maßnahmen den Patienten unmittelbar in seiner Privatsphäre. Deshalb und wegen der möglichen erheblichen Bedeutung der in solchen Unterlagen enthaltenen Informationen für selbstbestimmte Entscheidungen des Behandelten habe dieser ein geschütztes Interesse daran zu erfahren, wie mit seiner Gesundheit umgegangen worden sei, welche Daten sich dabei ergeben hätten und wie man die weitere Entwicklung einschätze. Das Bundesverfassungsgericht hat hervorgehoben, dass dieser grundrechtlich verankerte Anspruch auch dann besteht, wenn der Patient im Strafvollzug oder Maßregelvollzug untergebracht ist. Diese Personengruppe könne ihren Arzt nicht frei wählen. Zudem sei der Vollzug durch ein besonders hohes Machtgefälle zwischen den Beteiligten geprägt, weshalb die Grundrechte der Betroffenen naturgemäß besonderer Gefährdung ausgesetzt seien. Dies gelte auch in Bezug auf die Führung der Akten und den Zugang zu ihnen. Der Inhalt der Krankenunterlagen sei wegen seines sehr privaten Charakters in besonderem Maße grundrechtsrelevant. Ohne Akteneinsicht könne sich der Betroffene nicht vergewissern, ob die Aktenführung den grundrechtlichen Anforderungen entspreche, und seinen Anspruch auf Löschung oder Berichtigung falscher Informationen nicht in gleicher Weise verwirklichen.

Die Änderung nach § 185 StVollzG-E wonach die betroffene Person Akteneinsicht erhält, wenn ihr ein Recht auf Auskunft zusteht, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht und sie hierfür auf die Einsichtnahme angewiesen ist, genügt diesen Anforderungen nicht.

d) § 88 StVollzG: besondere Sicherungsmaßnahmen

In § 88 Abs. 2 Nummer 2 StVollzG sollten die Wörter „bei Nacht“ durch die Wörter „auch mit technischen Hilfsmitteln“ ersetzt werden.

Die Bestimmung ermöglicht auch im Vollzug der Haft nach § 171 StVollzG eine Beobachtung der Gefangenen mit technischen Hilfsmitteln und stellt die Zivilgefangenen damit den Strafgefangenen gleich, da eine solche Möglichkeit in den Landesstrafvollzugsgesetzen vorgesehen ist. Eine derartige Überwachung ist insbesondere in den Fällen einer akuten Gefahr der Selbsttötung erforderlich.

Dr. Georg Gieg
Richter am Oberlandesgericht

Stellungnahme

zum Gesetzentwurf der Bundesregierung vom 01.10.2018 eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 vom 27.04.2016 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 - BT-Drucksache 19/4671)

(Stand: 18.02.2019)

Ich halte den Gesetzesentwurf der Bundesregierung für einen mehr als beachtlichen und angesichts der Komplexität und des Umfangs der Aufgabe ganz überwiegend inhaltlich wie handwerklich gelungenen Entwurf.

Die Schwierigkeit besteht nicht nur darin, das ‚neue Recht' angesichts der gerade in der StPO ‚gepflegten', mitunter anstrengenden Verweisungstechnik auf andere Bestimmungen desselben Gesetzes umzusetzen. Hinzu kommt, dass in dieses für den Normanwender ohnehin komplexe Geflecht die Anforderungen insbesondere der Richtlinie (EU) 2016/680 vom 27.04.2016 einzuweben und dabei überdies die (neue) Datenschutzgrundverordnung und das Bundesdatenschutzgesetz (BDSG 2018) nicht aus den Augen zu verlieren.

Dass der durchgängig mit spürbarer Bedachtsamkeit begründete Entwurf dennoch im Wesentlichen als ‚deutsches Verfahrensrecht' wiedererkennbar bleibt, ist ebenso erfreulich wie die für die Akzeptanz des vorgesehenen Regelwerks nicht minder bedeutsame Umsetzung zentraler Anliegen der Rechtsprechung des Bundesverfassungsgerichts.

So wird nach meiner Überzeugung etwa allein und unabhängig vom diskussionswürdigen Standort im Gesetz und weiteren Einzelfragen die Verankerung des für eingriffsintensive Überwachungs- und Ermittlungsmaßnahmen vom Bundesverfassungsgericht (vgl. statt aller BVerfG [1. Senat], Urteil vom 20.04.2016 – 1 BvR 966/09 u.a. = BVerfGE 141, 220-378 [insbesondere Rn. 275 ff.] = EuGRZ 2016, 149 = NJW 2016, 1781 = StV 2016, 43 = DuD 2016, 469 = BayVBl 2016, 589 = CR 2016, 796 m.w.N.) geforderten ausfüllenden ‚Schranken-Schranke-Kriteriums' der „hypothetischen Datenneuerhebung"

in Anknüpfung an das vertraute Merkmal des „hypothetischen Ersatzeingriffs“ der Anwendungspraxis wesentliche Orientierungshilfen mit Strahlkraft auf die Gesamtmaterie geben können.

Denn die Entscheidung darüber, ob von einer nach den Grundsätzen der Zweckbindung und Zweckänderung noch erlaubten oder aber nicht mehr erlaubten Datennutzung auszugehen ist, kann dem Normanwender bei der in jedem Einzelfall im Rahmen der Verhältnismäßigkeitsprüfung gebotenen Abwägung über die Schaffung hinreichend gängiger „Doppeltüren“ als Rechtsgrundlagen hinaus vom Gesetzgeber nicht abgenommen werden (zum Leitbild des sog. ‚Doppeltürmodells‘ vgl. rechtsgrundsätzlich BVerfG, Beschl. v. 24.1.2012 – 1 BvR 1299/05 = BVerfGE 130, 151, 184 = NJW 2012, 1419 = CR 2012, 245 = DuD 2012, 532; instruktiv u.a. auch BVerfG [3. Kammer des 1. Senats], Beschl. v. 6.3.2014 – 1 BvR 3541/13 = NJW 2014, 1581 = StV 2015, 469).

In der Gesamtschau gelingt dem Entwurf insoweit bei der Umsetzung des anspruchsvollen Änderungsanlasses in ambitionierter Art und Weise die für jedwede Normakzeptanz unabdingbar notwendige Nachvollziehbarkeit des vorgesehenen Regelwerks auf schwierigem Terrain, ohne hierbei das im deutschen Recht verbürgte Datenschutzniveau für natürliche Personen herabzusetzen.

Dr. Georg Gieg

Vereinigung
Berliner
Strafverteidiger e.V.

Vereinigung Berliner Strafverteidiger e.V. Meinekestraße 3, 10719 Berlin

Deutscher Bundestag

Ausschuss für Recht & Verbraucherschutz

Herrn Vorsitzenden Brandner, MdB

Meineke Straße 3
10719 Berlin
Telefon 030-347 812 65
Telefax 030-347 812 66
www.strafverteidiger-berlin.de
email@strafverteidiger-berlin.de

Postbank Berlin
BLZ 100 100 10
Konto 660 81-103

IBAN DE55 1001 0010 0066 0811 03
BIC: PBNKDEFF

Berlin, 20. Februar 2019

Stellungnahme in der 37. Sitzung des Rechtsausschusses des Bundestages zum Gesetzesentwurf 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

I. Vorab

Grundsätzlich ist die weitere Konkretisierung der Vorgaben der Datenschutzgrundverordnung in das nationale Strafverfahrensrecht zu begrüßen. Der Gesetzesbegründung ist zu entnehmen, dass eine formell ernstgemeinte Umsetzung des auf Ebene der Europäischen Union etablierten Datenschutzes angestrebt wird, und man sich im Bereich des Strafverfahrensrechts der Ambivalenz zwischen dem staatlichen Anspruch bewusst ist, einerseits auch im Geheimen ermitteln zu dürfen, also Daten zu erheben, andererseits aber Instrumente in die Gesetze zu verankern, die den Betroffenen die Sicherung und Ausübung ihrer datenschutzrechtlichen Rechte ermöglicht.

Begrüßt wird ausdrücklich, dass das auf EU-Ebene bestehende Verbot des Profilings übernommen wird bzw. die JR-Richtlinie eine Definition hierzu enthält.

Vorangestellt wird der ausdrückliche Hinweis darauf, dass Artikel 1 Absatz 3 der Richtlinie es den Mitgliedstaaten erlaubt, strengere Regeln zum Datenschutz zu nomieren und die Bundesrepublik Deutschland das als Ansporn verstehen sollte, den innerdeutschen Datenschutz weiter zu entwickeln.

Soweit ein besserer Datenschutz allerdings der Begründung zufolge etabliertt werden soll, um gerade den transnatioaneln Datenverkehr – insbeondere auch in Drittstaaten – zu erleichtern, ist zu kritisieren, dass der formell immer weitergehende Datenschutz in-der Praxis auch umzusetzen ist – was aus meiner Sicht als Forensikerin nicht der Fall ist - und hierfür die entsprechenden Mittel zur Verfügung gestellt werden müssen.

II. Rechtliches

In gebotener Kürze beschränke ich meine Kritik des Gesetzesentwurfs auf die Punkte Anwendungskonkurrenz (hierzu unter 1.), fehlende Stringenz anderer datenschutzerheblicher Regelungen zur angestrebten Gesetzesänderung (hierzu unter 2.) und Fragen der Löschungspflicht (hierzu unter 3.)

1. Anwendungskonkurrenz

Bereits in der Gesetzesbegründung sind komplexe Ausführungen dazu enthalten, welches Datenschutzrecht anwendbar ist und wie sich die Anwendungsvorgaben zu den Regelungen im Bundesdatenschutzgesetz (2018) als insoweit so benannte allgemeine Reglungen zu in der StPO (und damit verwandten Regelungen) enthaltenen bereichsspezifischen Sonderreglungen verhalten soll. Vorgegeben wird – juristisch unüblich – die Geltung des 3. Teils des BDSG (2018) als allgemeine Regelungen und dazu die ergänzende Prüfung, ob bereichsspezifische Regelungen in der StPO enthalten sind (Begründung S. 44). Diese Anwendungsvorgabe wird zu Recht als *„neuartiges Regelungsgefüge“* bezeichnet, was die Handhabung der Regelungen erschweren wird - gerade für Strafjuristen, die nicht explizit im (neuen) Datenschutzrecht ausgebildet sind.

Auch wenn zur Vorgabe des zunächst anzuwendendes Recht Klarstellungen und ergänzende Reglungen im Gesetzesentwurf vorgeschlagen worden sind, zum Beispiel die Übernahme des § 160 Abs. 4 StPO in § 161 Absatz 1, S. 3 StPO, oder auch Anwendungsvorgaben in den RiStBV, so ist das vom dem Gesetzesentwurf angedachte Gesetzesgefü-

ge kompliziert und trägt gerade nicht zur Sensibilisierung im unter anderem Bereich der Datensparsamkeit bei.

Der Gesetzgeber sollte aufgefordert werden, eine klarere Struktur zum Verhältnis der datenschutzrechtlichen Normen zu etablieren, die die Gesetzesanwendung erleichert, und beispielsweise mit mehr Verweisungen dort zu arbeiten, wo er die Regelungen des Bundesdatenschutzrechts als vorrangig angwendet wissen will.

2. Fehlende Stringenz bei vom Datenschutz betroffenen Regelungen

Hieran anknüpfend wird darauf verwiesen, dass die StPO bereits umfangreiche Regelungen zur Verwendung von Daten, zum Beispiel Akteneinsichtsrechte für den Beschudigten, aber auch unter anderem dem Nebenkläger oder – weitergehender – dem Verletzten hat, vgl. unter anderem §§ 406d StPO.

Dem Gesetzentwurf und seiner Begründung zufolge sollen diese Rechte neben den beispielweise Auskunftsrechten des BDSG bestehen bzw. diese nicht verdrängen (u. a. Änderungen zu Nummer 19, §§ 475 Absatz 1 Satz 1 StPO, § 57 BDSG, Entwurf Seite 67), was im Ergebnis eine Erweiterung von Auskunftsrechten von Dritten bedeutet, die nicht Nebenkläger, Verletzte u. Ä. sind.

In dieser Konstellation lässt der Gesetzesentwurf nicht erkennen, ob er sich der damit verbundenden Betroffenheit der datenschutzrechtlichen Interessen des eigentlichen Subjekts im Strafverfahren bewusst ist. Der zu erkennende gesetzgeberische Wille erschöpft sich in der Beachtung der Rechte von Dritten ohne die damit zwingend verbundenen Eingriffe der Rechte des eigentlich von einem Strafverfahren Betroffenen zu beachten bzw. zu verhindern.

3. Löschungspflicht

Die im Datenschutzrecht im Allgemeinen und in der StPO besonderen Regelungen zu Löschungspflichten dokumentieren das Spannungsverhältnis zwischen dem staatlichen Anspruch auf geheime Ermittlungen einerseits und Auskunftsrechten andererseits. Sie sind ebenfalls sehr komplex gehalten und die im Gesetzesentwurf angedachten Verweise werden die Rechtsanwendung nicht erleichtern.

Beispielsweise wird das Recht auf Berichtigung, Löschung und Einschränkung der Bearbeitung konterkariert, wenn – wie in § 58 Absatz 3 Nr. 3 BDSG – geregelt die Löschung unterbleiben kann, wenn sie einen unverhältnismäßigen Aufwand bedeutet. Artikel 16 der Richtlinie sieht eine solche Regelung nicht vor; § 58 Absatz 3 S. 3 BDSG ist nicht richtlinienkonform und sollte im Strafverfahrensrecht nicht gelten.

Die Löschungspflichten sollten weiter an dem Prinzip der Erforderlichkeit der Speicherung festhalten bzw. diese stärker gegenüber den Möglichkeiten der einschränkenden und archivierenden Speicherung gewichten. Anderenfall droht eine Praxis, die gerade nicht den Grundsatz der Datensparsamkeit lebt, sondern Daten dem Vorsichtsprinzip folgend zwar einschränkend speichert, aber immer noch speichert. Dadurch wird die Angst um einen Datenverlust geschützt, anstatt für den sorgvollen Umgang und die dazugehörende Löschung von Datern zu sensibilisieren.

Nicht zuletzt laufen die geregelten Auskunfts- und Löschungsrechte u. Ä. leer, wenn die Betroffenen nicht ausreichend über ihre Rechte informiert werden (siehe unten), oder Verstöße gerade nicht Betroffenen, sondern der Aufsichtsstelle gemeldet werden müssen; die Vorgaben des Artikel 12 Absatz 2 sind nicht ausreichend umgesetzt. In diesem Zusammenhang ist auch die Regelung eines kollektiven Rechtsschutzs zu fordern, wie Art. 52 ff. der Richtlinie ihn vorsehen.

III. Praktisches

Die Gesetzesbegründung benennt zur Umsetzung der Richtlinie wie im Entwurf vorgeschlagen, einen geringen Aufwand und unterbreitet beispielsweise die nicht erklärte Berechnung, wonach in ca. 1 % der bei der Staatsanwaltschaft anhängigen Verfahren mit Auskunftsersuchen zu rechnen ist und ein Staatsanwalt zur Prüfung dieses Ersuchens ca. 20 Minuten aufbringen wird.

Diese Annahme ignoriert die komplexe Gesetzesmaterie wie zum Beispiel zur Anwendungskonkurrenz aufgezeigt und im Übrigen den forensischen Alltag. Dieser zeichnet sich unter anderem dadurch aus, dass selbst zu den in der StPO geregelten Akteneinsichtsrechten von grundsätzlich Prozessbeteiligten (siehe unter II.2.) keine Sensibilisierung

betreffend die Herausgabe von Daten an Dritte zu brobachten ist, beispielsweise solche oftmals ohne vorherige Gewährung rechtlichen Gehörs zugunsten des Beschuldigten erfolgen, Akteneinsichten an unter anderem Insolvenzverwalter gewährt werden, ohne dass von diesen das gesetzlich geforderte berechtigte Interesse gelten gemacht wird usw.

Ein Googleversuch hat im Übrigen ergeben, dass das Landgericht Berlin beispielhaft gerade nicht mit *„einem Klick“* auffindbar über die Verwendung von Daten und den Rechten der Betroffenen informiert, meiner Kenntnis nach auch keine entsprechenden Aushänge im Kriminalgericht hierüber informieren, erst recht nicht in einfacher Sprache.

IV. Zusammenfassung

Die mit dem Gesetzesvorhaben bezweckte Stärkung der Datenschutzrechte von Betroffenen im Strafverfahren wird nicht eintreten, solange der Justiz nicht weitergehende Ressourcen zur Verfügung gestellt werden und die Verantwortlichen nicht sichtbarer über den Datenschutz sensibilisiert werden.

Halbritter
Rechtsanwältin

Matthias Kegel
Oberstaatsanwalt
Generalstaatsanwaltschaft
des Landes Brandenburg

Brandenburg a.d.H., den 18.02.2019

- per E-Mail –

An den
Deutschen Bundestag
Ausschuss für Recht
und Verbraucherschutz
Sekretariat PA 6

Öffentliche Anhörung

des Ausschusses für Recht und Verbraucherschutz

des Deutschen Bundestages

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)

am 20.02.2019

Zum vorliegenden Gesetzentwurf nehme ich wie folgt Stellung:

Artikel 1 Nummer 6 a bb: § 100g Absatz 1 Sätze 3 und 4 StPO-E

Die neuen Sätze 3 und 4 in § 100g Absatz 1 StPO-E erlauben die Erhebung der aus betrieblichen Gründen gespeicherten (retrograden) Standortdaten nach § 96 Absatz 1 TKG. Die Regelung ist unbedenklich; sie widerspricht weder der Intention des Gesetzgebers aus 2015, noch werden damit die Befugnisse der Strafverfolgungsbehörden erweitert. Vielmehr wird dadurch eine nicht vorhersehbare planwidrige Vollzugslücke geschlossen.

Standortdaten dürfen in Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 02.03.2010 (NJW 2010, 833) nur noch in den engen Grenzen von § 100g Absatz 2 StPO aus den Vorratsdaten nach § 113b TKG erhoben werden. Bereits im Zeitpunkt des Inkrafttretens des „Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ am 18.12.2015 bestand in Bezug auf die Erhebung von Standortdaten eine Vollzugslücke, weil die Pflicht zur Speicherung dieser Daten nach § 113b Absatz 4 TKG für die Provider nach der Übergangsregelung des § 150 Absatz 13 TKG erst zum 01.07.2017 gegriffen hat und in dieser Zeitspanne die Erhebung von Standortdaten nach § 100g Absatz 2 StPO ins Leere gelaufen wäre. Der Gesetzgeber wollte hingegen einen lückenlosen retrograden Abruf von Standortdaten beim Verdacht auf Begehung einer Katalogstraftat nach § 100g Absatz 2 StPO (BT-Drs. 18/5088, S. 44) ermöglichen. Diese Lücke schloss er mit einer Übergangsregelung in § 12 Absatz 1 EGStPO, wonach die nach § 96 Absatz 1 Satz 1 Nummer 1 TKG gespeicherten Standortdaten bis zum 29.07.2017 auf der Grundlage des § 100g Absatz 1 StPO in der bisherigen Fassung erhoben werden durften.

Faktisch bestand auch nach dem 01.07.2017 ein Vollzugshemmnis fort, was dazu führte, dass die Staatsanwaltschaften Standortdaten nach § 113b Absatz 4 TKG weiterhin nicht erheben konnten. Denn fast alle Provider speichern überhaupt keine Vorratsdaten mehr, nachdem die Bundesnetzagentur am 28.06.2017 unter Hinweis auf die Entscheidung des OVG Münster vom 22.06.2017 (Az. 13 B 238/17, BeckRS 2017, 114873) und das Urteil des EuGH vom 21.12.2016 (NJW 2017, 717) erklärt hat, keine Anordnungen und sonstige Maßnahmen zur Durchsetzung der Speicherverpflichtung gegen Provider zu ergreifen. Damit wird die Aufklärung von schweren Straftaten erschwert, wenn nicht gar verhindert. Die Justizministerinnen und Justiz-

minister haben auf ihrer Herbstkonferenz am 09.11.2017 daher den Gesetzgeber aufgefordert, Sorge zu tragen, dass den Strafverfolgungsbehörden weiterhin der Zugriff auf von den Dienstanbietern gespeicherte Standortdaten ermöglicht wird.

Wie zuvor in 2015 wird der gesetzgeberische Wille nach einer lückenlosen Erhebung der Standortdaten durch die Neuregelung in § 100g Absatz 1 Satz 3 und 4 StPO-E geschlossen, indem die Strafverfolgungsbehörden die nach § 96 Absatz 1 Satz 1 Nummer 1 TKG gespeicherten Standortdaten unter den Voraussetzungen des § 100g Absatz 2 StPO-E erheben dürfen.

Artikel 1 Nummer 35: § 491 StPO-E

Nach der Neuregung von § 491 StPO-E entfallen nach Antrag durch die betroffenen Personen die Sperrfristen für die Auskunft zu laufenden Verfahren und der pauschale Hinweis bei einer Negativauskunft auf diese Sperrfristen nach § 491 Absatz 1 Satz 2 bis 6 StPO. Damit wird (zum Leidwesen insbesondere der staatsanwaltschaftlichen Praxis wegen des damit verbundenen Mehraufwandes) konsequent Artikel 14 der Richtlinie (EU) 2016/680 umgesetzt, der solche Sperrfristen nicht kennt. § 491 StPO-E gilt nur noch subsidiär zum Auskunftsanspruch der betroffenen Personen nach § 57 BDSG.

Das BMJV hat in der Abstimmung zu den Referentenentwürfen die Einwände aus der staatsanwaltschaftlichen Praxis in § 491 Absatz 2 Satz 2 StPO-E aufgegriffen, um der Gefahr einer Ausforschung des staatsanwaltschaftlichen Fachverfahrens zu begegnen, indem der Bescheid an die antragstellende Person keinen Rückschluss zulassen soll, ob noch geheim zu haltende Ermittlungsverfahren vorliegen oder nicht, um den Ermittlungserfolg nicht zu gefährden. Dadurch wird die bisherige Auskunftserteilung – bis auf die Sperrfristen – beibehalten.

Artikel 1 Nummer 41: § 500 StPO-E

Dass Teil 3 des Bundesdatenschutzgesetzes auf das gesamte Strafverfahren für alle öffentlichen Stellen der Länder anzuwenden ist, wird ausdrücklich begrüßt. Damit wird ein einheitlicher Datenschutzstandard bei Gerichten, Strafverfolgungsbehörden, Vollstreckungsbehörden, Bewährungshilfe, Aufsichtsstellen bei Führungsaufsicht und Gerichtshilfe gewährleistet, eine länderspezifische Zersplitterung vermieden und alle betroffenen Personen datenschutzrechtlich gleich behandelt.

Würden hingegen die jeweiligen Landesdatenschutzgesetze für Staatsanwaltschaften, Gerichte und Polizei zur Anwendung gelangen, wäre das mit nicht unerheblichen Nachteilen verbunden, weil die Länder bereits im Gesetzgebungsverfahren begonnen hatten, die Richtlinie (EU) 2016/680 für Justiz und Polizei in den Landesdatenschutzgesetzen mit differenzierenden Regelungen von Bundesland zu Bundesland zu integrieren.

a) Eine länderspezifische Zersplitterung würde in den länderübergreifenden Fachverfahren zu schwierigen länderspezifischen Anpassungsprogrammierungen führen. Neben dem zusätzlichen personellen und finanziellen Aufwand wäre die Weiterentwicklung der Fachverfahren kaum mehr zu beherrschen.

b) Die länderübergreifende Kommunikation und der länderübergreifende Datenaustausch in Strafsachen bei elektronischer Aktenführung wären durch eine unterschiedliche datenschutzrechtliche Ausgestaltung in den einzelnen Bundesländern erschwert. Die Kommunikationsszenarien müssten diese Unterschiede berücksichtigen. Das würde dem Bestreben aus dem Koalitionsvertrag zuwiderlaufen, den Datenaustausch im Bereich der Strafverfolgung zwischen Polizei und Justiz verbessern zu wollen (S. 123, Zeile 5767 f.).

Der Verbleib der Zuständigkeit der Datenschutzaufsicht bei den Landesbeauftragten gewährleistet im Übrigen eine einheitliche Aufsicht der Staatsanwaltschaften und der übrigen öffentlichen Stellen in den jeweiligen Bundesländern.

Artikel 2: § 17 EGStPO-E

Die IT-Anwendungen der Staatsanwaltschaften und Gerichte sind nicht in der Lage, die datenschutzrechtlichen Anforderungen kurzfristig umzusetzen. Die entsprechenden Hinweise der Landesjustizverwaltungen sind in § 17 Absatz 3 EGStPO aufgegriffen worden, wonach für die IT-Anwendungen der Staatsanwaltschaften und Gerichte längere Umsetzungsfristen nach Artikel 63 Absatz 2 und 3 der Richtlinie (EU) 2016/680 gelten sollen, um hinreichend Zeit für die Umsetzung der neuen Protokollierungsvorgaben und die hierfür erforderlichen technischen Anpassungen einzuräumen.

gez.
Matthias Kegel
Oberstaatsanwalt

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

OStA b BGH Dr. Moldenhauer

Schriftliche Stellungnahme
zu der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages am 20. Februar 2019

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

Der Gesetzentwurf regelt in § 161 Abs. 3 und Abs. 4 StPO-E die Verwendung von Daten, die nach anderen Gesetzen erhoben wurden, und in § 479 Abs. 2 StPO-E die Verwendung der sogenannten Zufallsfunde jeweils neu.

Die Neuregelung wird im Wesentlichen dadurch erreicht, dass die Worte „zu Beweiszwecken" in den geltenden § 161 Abs. 2 und § 477 Abs. 2 StPO gestrichen werden. Im Ergebnis ist so jegliche Verwendung von Daten, die mit bestimmten eingriffsintensiven Mitteln erhoben wurden, nur zur Aufklärung von Straftaten möglich, für die eine solche eingriffsintensive Maßnahme auch nach der StPO jeweils angeordnet werden könnte oder bei „vergleichbar bedeutenden Straftaten".

I)

Die Generalklausel für staatsanwaltschaftliche Ermittlungen, § 161 StPO, soll durch den Gesetzentwurf in Abs. 3 und Abs. 4 Regelungen für die Verwendung von Daten erhalten, die auf Grund *eines anderen Gesetzes*, also nicht auf Grund strafprozessualer Maßnahmen, erhoben wurden. Anknüpfungspunkt für eine solche Verwendung ist – sofern keine Katalogtat vorliegt – die „Aufklärung jeweils vergleichbar bedeutender Straftaten".

Diese Formulierung trägt zunächst nicht zur Normklarheit bei. Es sei auf die Diskussion hinsichtlich des Begriffs der „Straftat von erheblicher Bedeutung" hingewiesen (vgl. BVerfG, Urteil vom 27.07.2005 – 1 BvR 668/04, BVerfGE 113, 348, Rn. 154ff.; Moldenhauer in: Karlsruher Kommentar zur StPO, 7. Auflage, § 163e Rn. 13). Zwar könnte sich hier eine Konkretisierung möglicherweise daraus ergeben, dass bei einem Teil der Eingriffsmaßnahmen nach der Strafprozessordnung – etwa in § 100a Abs. 2 StPO – ein Straftatenkatalog vorgesehen ist, dies ist aber nicht durchgehend der Fall, vgl. etwa §§ 100i, 110a, 163e StPO. Im Übrigen drängt sich die Frage auf, warum die „vergleichbar bedeutende Straftat" nicht von vornherein in den Katalog aufgenommen wurde.

II)

Die Verwendung von Daten als Spurenansatz wird in der Praxis erheblich eingeschränkt werden. Das den Strafprozess prägende Legalitätsprinzip (§ 152 Abs. 2 StPO) wird in vielen Fällen leerlaufen. Im Einzelnen:

1) Die Umsetzung im Gesetzentwurf beruht auf der Entscheidung des Bundesverfassungsgerichts zum BKAG (vgl. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, BVerfGE 141, 220ff., Rn. 315). Danach ist fraglich, ob § 161 StPO der verfassungsrechtlich gebotenen Begrenzung der zweckändernden Datennutzung – bezogen auf polizeipräventive Daten – ausreichend Rechnung trägt.

Rechtspraktisch wird durch die Neuregelung sehr wahrscheinlich insbesondere ein Teil der polizeipräventiven Zufallserkenntnisse der Strafverfolgung nicht zugänglich sein.

2) Gravierender – und mE in der Form nicht geboten – ist die Einführung des § 479 Abs. 2 StPO-E. Dieser verweist nun für sämtliche Daten, die auf Grund der Strafprozessordnung erhoben wurden, auf § 161 Abs. 3 und Abs. 4 StPO-E. Die Regelung setzt damit den strafprozessualen Zufallsfund den Maßnahmen *aus anderen Gesetzen* gleich und entzieht ihn, sofern er keine Katalogtat oder „vergleichbar bedeutende Straftat" betrifft, ebenfalls der Strafverfolgung. Das widerspricht tradierten strafprozessualen Grundsätzen und geht über die durch das Bundesverfassungsgericht und die DSGVO aufgestellten Anforderungen hinaus.

Grundsätzlich können bei eingriffsintensiven Maßnahmen, wie beispielsweise bei der Telekommunikationsüberwachung nach § 100a StPO, nicht Katalogtaten betreffende Zufallsfunde zwar nicht zu Beweiszwecken verwertet werden. Sie können aber als Ermittlungsansatz in weiteren Verfahren verwendet werden (vgl. Meyer-Goßner/Schmitt, StPO, 61. Aufl., § 477 Rn. 5aff. m.w.N). Dies ist durch das Bundesverfassungsgericht anerkannt (vgl. BVerfG, Beschluss vom 26. Juni 2005 – 2 BvR 866/05, NJW 2005, 2766). Etwas anderes gilt nur für die spezialgesetzlichen Regelungen der akustischen Wohnraumüberwachung und der Onlinedurchsuchung (vgl. § 100e Abs. VI StPO), was im Hinblick auf die unterschiedliche Eingriffstiefe einleuchtet.

Es ist anerkannt, dass eine Verwendung der Erkenntnisse als Ermittlungsansatz zwar zu einer Wiederholung oder Vertiefung des Grundrechtseingriffes führt, weil die Daten in weiterem Umfang von Verfahrensbeteiligten zur Kenntnis genommen werden. Das Schwergewicht des Eingriffes liegt gleichwohl nicht in dieser weiteren Verwendung der Überwachungsergebnisse, sondern im vorangehenden, bereits abgeschlossenen Ermittlungsgeschehen, für das eine rechtfertigende Ermächtigungsgrundlage gegeben war (vgl. Allgayer, NStZ 2006, 603, 606).

Die in § 479 Abs. 2 StPO-E vorgesehene Verwendungsbeschränkung bei rechtmäßig erhobenen Daten geht letztlich weiter als bei Verwertungsbeschränkungen aus rechtswidrigen Maßnahmen. Dem Strafverfahrensrecht ist ein allgemein geltender Grundsatz wesensfremd, demzufolge jeder Verstoß gegen Beweiserhebungsvorschriften ein strafprozessuales Verwertungsverbot nach sich zieht. Die Frage der Verwertbarkeit ist jeweils nach den Umständen des Einzelfalls, insbesondere nach der Art des Verbots und dem Gewicht des Verstoßes, unter Abwägung der widerstreitenden Interessen zu entscheiden (vgl. BVerfG, Beschluss vom 9. 11. 2010 − 2 BvR 2101/09, NJW 2011, 2417, 2418).

Die in § 479 Abs. 2 StPO-E vorgesehene Einschränkung des Ermittlungsansatzes bei Zufallsfunden birgt die Gefahr der „Rechtserosion" in sich. Die Strafverfolgungsbehörden werden hinnehmen müssen, dass sie vielfach ihrem durch Legalität und Amtsaufklärung geprägten gesetzlichen Auftrag nicht nachkommen können. Ergeben sich zum Beispiel aus einem beim Generalbundesanwalt geführten Ermittlungsverfahrens wegen Mitgliedschaft in einer terroristischen Vereinigung (§ 129a StGB) im Rahmen von Telekommunikationsüberwachungsmaßnahmen (§ 100a StPO) singulär Hinweise auf den Verdacht der Volksverhetzung (§ 130 Abs. 1 StGB) und des Aufbruchs eines

Kraftfahrzeuges (§§ 242, 243 Abs. 1 Nr. 1 StGB) gegen einen nicht Tatbeteiligten, so könnten diese Erkenntnisse nach § 479 Abs. 2 StPO-E in Verbindung mit § 161 Abs. 3 Nr. 1 StPO-E nicht für die weitere Aufklärung als Spurenansatz verwertet werden. Es handelt sich weder um Katalogtaten noch um „vergleichbar bedeutende Straftaten“ im Sinne des § 161 Abs. 3 Nr. 1 StPO-E.

Der Bayerische Landesbeauftragte für den Datenschutz

Bayer. Datenschutzbeauftragter • PF 22 12 19 • 80502 München

Deutscher Bundestag
Ausschuss für Recht und Verbraucherschutz
Platz der Republik 1
11011 Berlin

vorzimmer.pa6@bundestag.de

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen	München, den 18.02.2019
	DSB/566-205-16	Durchwahl: 089 212672 - 0

Öffentliche Anhörung des Ausschusses für Recht und Verbraucherschutz am 20.02.2019
Umsetzung europäischen Datenschutzrechts im (Straf)Verfahrensrecht

Sehr geehrte Mitglieder des Ausschusses für Recht und Verbraucherschutz,

für die Gelegenheit zur Stellungnahme bedanke ich mich und konzentriere mich auf die geplante Änderung der Strafprozessordnung. In vielen Punkten teile ich dabei die Einschätzungen der vormaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 16.11.2018. Ich verzichte insoweit weitgehend auf eine redundante Darstellung und möchte lediglich auf einige wenige Punkte aufmerksam machen, die mir aus Sicht der Datenschutzaufsichtsbehörde eines Bundeslandes wichtig sind.

Dies vorweg geschickt, vermisse ich eine vollständige Umsetzung der Richtlinie EU 2016/680. Nach seinem Maßstab für die Umsetzung dieser Richtlinie sieht der Gesetzentwurf in der StPO keine umfassende Regelung der Verarbeitung personenbezogener Daten vor. Er beschränkt sich vielmehr darauf, einige wenige Vorschriften abzuändern. Soweit diese Änderungen des bereichsspezifischen Rechts nicht einschlägig sind, verweist der Entwurf auf die Auffangregelungen des BDSG 2018 (vgl. z.B. BT-Drs. 19/4671, S. 44).

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München

Telefon: 089 212672-0
Telefax: 089 212672-50
https://www.datenschutz-bayern.de
E-Mail: poststelle@datenschutz-bayern.de

Verkehrsverbindungen:
U4/U5, Haltestelle Lehel
Bus Linie 100, Straßenbahn Linie 18
Haltestelle Nationalmuseum / Haus der Kunst

Dagegen ist im Grundsatz zwar nichts einzuwenden. Kritikwürdig ist aber, dass der Gesetzentwurf abgesehen von einigen Detailregelungen ausschließlich die Vorschriften des Achten Buchs einer relativ gewissenhaften Revision unterzogen hat. Nach meiner Einschätzung ist es jedoch auch erforderlich, jedenfalls die Vorschriften des sechsten, siebten und achten Abschnitts des ersten Buches eingehender auf einen Umsetzungsbedarf zu überprüfen und gegebenenfalls zu ändern. Der Gesetzentwurf sieht insoweit im Wesentlichen nur redaktionelle Änderungen vor oder Änderungen, die selten in einem Zusammenhang mit der Umsetzung der Richtlinie stehen.

Für mich gut nachvollziehbar hat die Bundesbeauftragte für den Datenschutz beispielhaft darauf hingewiesen, dass die StPO bislang **keine Rechtsgrundlage für Datenerhebungen durch sog. V-Leute** vorsieht und dass dies einen rechtsstaatlichen Mangel darstellt. In diesem Zusammenhang mache ich ergänzend darauf aufmerksam, dass der Bayerische Polizeigesetzgeber für die präventivpolizeiliche Datenerhebung durch V-Leute eine gesetzliche Verarbeitungsgrundlage für rechtsstaatlich geboten angesehen und mit Art. 38 Polizeiaufgabengesetz auch geschaffen hat. Zur Begründung führte der Bayerische Gesetzgeber unter anderem aus, dass „in Anbetracht der Maßgaben des BVerfG im BKAG-Urteil (Rn. 172 ff. und 358) … sowie insgesamt des im Vergleich zur Vergangenheit gesteigerten rechtspraktischen Regelungserfordernisses … nunmehr eine eigenständige präventivpolizeiliche Vorschrift in das PAG aufgenommen“ (BayLT-Drs. 17/20425, S. 56) wird.
Ebenso hat er bereits 2016 im Bayerischen Verfassungsschutzgesetz eine entsprechende Rechtgrundlage für den Einsatz von V-Leuten (Art. 19 BayVSG) eingeführt.

Ich empfehle,

> **die praktische Notwendigkeit von Datenerhebungen durch V-Leute kritisch zu überprüfen.**
> **Falls der Gesetzgeber auch für die Zukunft derartige Datenerhebungen für geboten hält, sollte er auch eine entsprechende Verarbeitungsgrundlage schaffen.**

Im Übrigen bitte ich um Nachsicht, dass ich in der Kürze der mir zur Verfügungen gestellten Zeit keine umfassende Analyse des Umsetzungsbedarfs der Abschnitte 6 bis 8 des Ersten Buches vorlegen konnte.

Wenigstens einige Beispiele möchte ich allerdings herausgreifen – auch weil ich insoweit eine Reihe von Fällen kenne, in denen betroffene Personen erhebliche Nachteile erlitten haben.

Der Gesetzentwurf stellt nicht ansatzweise Überlegungen an, ob und inwieweit man die **Informationspflichten** der Richtlinie auf die Regeln der Zeugenvernehmung übertragen kann. Als Zeuge in mehreren Strafverfahren habe ich es ungeachtet des § 48 StPO noch nie erlebt, dass ich darüber aufgeklärt wurde, wer möglicher Datenempfänger meiner protokollierten Aussagen sein kann. Ich als Jurist bin mir zwar durchaus im Klaren darüber gewesen, dass beispielsweise der Angeklagte durch Akteneinsicht von meiner Zeugenaussage Kenntnis erhalten kann. Derartiges Wissen kann der Gesetzgeber aber nicht generell für alle Zeuginnen und Zeugen unterstellen! Ich weiß, dass Strafverfolgungsbehörden derartigen Unterrichtungen sehr kritisch gegenüber stehen, weil sie einen Mehraufwand bedeuten und möglicherweise lästige Fragen der betroffenen Personen nach sich ziehen. Meines Erachtens sind solche Überlegungen allerdings keine triftigen Gründe, die nach Maßgabe des Art. 13 Abs. 2 Buchstabe c) der Richtlinie vorgegebenen Informationspflichten pauschal abzulehnen. Gerade Zeuginnen und Zeugen haben oft schutzwürdige Interessen zu erfahren, wofür ihre Aussagen gebraucht werden und vor allem, wer von diesen Aussagen Kenntnis erlangen kann. Natürlich habe ich nichts dagegen einzuwenden, wenn Strafverfolgungsbehörden nicht über etwaige Datenempfänger informieren, wenn und soweit sie damit zugleich den Zweck des Strafverfahrens gefährden würden. Art 13 Abs. 3 der Richtlinie EU 2016/680 sieht einige legitime Gründe vor, die Informationspflichten einschränken können. Aber die Unterrichtung über mögliche Datenempfänger pauschal auszublenden, wird der Grundsatzentscheidung für eine entsprechende Informationspflicht in Art. 13 der Richtlinie nicht gerecht. Auch § 56 BDSG, der über § 500 Abs. 1 StPO-Entwurf zukünftig zur Anwendung gelangt, hilft an dieser Stelle nicht weiter. Denn dieser setzt eine bereits bestehende Benachrichtigungspflicht betroffener Personen in fachgesetzlichen Regelungen voraus (BT-Drs. 18/11325, S. 112), ordnet diese aber nicht selbst an.

Ich empfehle,

> **die Abschnitte 6 bis 8 des Ersten Buchs der StPO im Hinblick auf eine effektive Gewährleistung von Betroffenenrechten einer Revision zu unterziehen.**

Auf eine weitere Besonderheit der Richtlinie EU 2016/680 möchte ich aufmerksam machen: Sie ist in Art. 8 Abs. 1 der Richtlinie zu finden. Er hat folgenden Wortlaut:

> *Die Mitgliedstaaten sehen vor, dass die Verarbeitung **nur** dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die von der zuständigen Behörde zu den in Art. 1 Abs. 1 genannten Zwecken wahrgenommen wird, und auf der Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt."*

Angesichts des eindeutigen Wortlauts sind andere Verarbeitungsgrundlagen von der Richtlinie nicht vorgesehen. **Namentlich die Einwilligung ist nach der Richtlinie nicht geeignet, als alleinige Verarbeitungsgrundlage zu dienen.** Dies ergibt sich unmissverständlich auch aus Erwägungsgrund 35 der Richtlinie. Er hebt darauf ab, dass die Einwilligung regelmäßig nicht freiwillig abgegeben wird und damit nicht wirksam sein kann.
Nach Erwägungsgrund 35 ist es den Mitgliedstaaten allenfalls möglich, durch Rechtsvorschriften vorzusehen, dass die betroffene Person einer Verarbeitung ihrer personenbezogenen Daten zu den Zwecken der Richtlinie zustimmen kann. Ich weise insoweit darauf hin, dass die Richtlinie an dieser Stelle bewusst nicht davon spricht, dass die betroffenen Personen „einwilligen", sondern dass sie „zustimmen" kann. Ich verstehe die Richtlinie EU 2016/680 so, dass eine Einwilligung als Verarbeitungsgrundlage nicht genügt, weil ihre Freiwilligkeit eben regelmäßig nicht gewährleistet ist. Dementsprechend ist die Zustimmung nur als „rechtsstaatliches Plus" zusätzlich zu einer gesetzlichen Verarbeitungsgrundlage denkbar.

Indessen verwendet die StPO den Begriff der Einwilligung wie selbstverständlich weiter. Eher zufällig werden drei Vorschriften geändert, die sich aber nicht auf die Einwilligung beziehen. Ich spreche von den §§ 155b Abs. 2 Satz 2, 161 Abs. 3 und 479 Abs. 2 und Abs. 3 StPO-Entwurf.

Mit EU-Datenschutzrecht möglicherweise noch vereinbar ist § 155b Abs. 2 Satz 2 StPO-Entwurf, der den Täter-Opfer-Ausgleich betrifft. Der Täter-Opfer-Ausgleich ist ein Verfahren, das von vorneherein auf die freiwillige Kooperation der Beteiligten (Verletzte und Beschuldigte) angewiesen ist. Eine zwangsweise Durchsetzung, wie sie in Erwägungsgrund 35 thematisiert wird, steht hier nicht im Raum.

Demgegenüber zielen § 161 Abs. 3 und § 479 Abs. 2 und Abs. 3 StPO-Entwurf auf die Nutzung von Ermittlungsbefugnissen ab. Insoweit steht die Freiwilligkeit der Einwilligungserklärungen grundlegend infrage.

Empfehlungen:

1. **Sämtliche Vorschriften der StPO, die unmittelbar auf Einwilligungen Bezug nehmen, sind darauf hin zu überprüfen, ob sie im Einklang mit den Vorgaben der Richtlinie EU 2016/680 stehen. Das ist typischerweise nicht der Fall, wenn die Einwilligungen dazu dienen sollen, eine gesetzliche Verarbeitungsgrundlage zu ersetzen bzw. deren Anwendungsbereich auszudehnen.**
2. **Namentlich die in § 161 Abs. 3 und in § 479 Abs. 2 und Abs. 3 StPO-Entwurf vorgesehenen Formulierungen „ohne Einwilligung der von der Maßnahme betroffenen Person“ sollten auf ihre Praxisrelevanz hin überprüft werden. Falls sie keine Relevanz aufweisen, sollten sie ersatzlos gestrichen werden.**
3. **Ergibt eine Prüfung, dass die Vorschriften insoweit in der Vollzugspraxis im Interesse der betroffenen Personen bedeutsam sind, sollte die Einwilligung durch das Recht der betroffenen Person ersetzt werden, im Antragswege die erlangten verwertbaren personenbezogenen Daten in ein (anderes) Strafverfahren einführen zu können.**

Eine letzte Anmerkung ist mir noch wichtig. § 489 StPO regelt die Berichtigung, Löschung und Sperrung von personenbezogenen Daten. § 489 Abs. 6 Satz 1 StPO (gegenwärtige Fassung) hat folgenden Wortlaut:

> *„Werden die Daten einer Person für ein weiteres Verfahren in einer Datei gespeichert, so unterbleibt die Löschung, bis für alle Eintragungen die Löschungsvoraussetzungen vorliegen.“*

Eine derartige Klausel wird als „**Mitziehklausel**“ bezeichnet: Die Speicherdauer sämtlicher erfassten Daten orientiert sich an dem Datum, das die längste Speicherfrist aufweist. Dieses Datum „zieht“ die anderen vorangegangenen Speicherereignisse nach. Aus datenschutzrechtlicher Sicht sind Mitziehklauseln generell nicht unproblematisch.
Die Bundesbeauftragte für den Datenschutz hat § 489 StPO für ihren Zuständigkeitsbereich für wenig praxisrelevant gehalten. Das kann ich aufgrund meiner Prüferfahrungen auf Landesebene in Bezug auf die Vollzugspraxis der Strafverfolgungsbehörden der Länder leider nicht bestätigen. Im Gegenteil: Die Vorschrift ist in meinem Zuständigkeitsbereich leider häufig und unglücklich angewandt worden. Mehrfach hatte ich Fälle zu beurteilen, die dem nachfolgenden Beispiel ähneln.

> Beispiel: Eine Person verübt einen Ladendiebstahl. Fünf Jahre später wird sie als Zeugin in einem Betrugsfall vernommen. Kurz vor Ablauf der Speicherfrist wird sie Opfer einer Körperverletzung, danach Zeugin eines Verkehrsunfalls, bei der sich ein Verkehrsteilnehmer strafbar macht. Alle diese Ereignisse führen dazu, dass die Speicherfrist der jeweils vorangegangen Ereignisse verlängert wird.

Ich halte § 489 Abs. 6 Satz 1 StPO (gegenwärtige Fassung) für einen unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der betroffenen Person. Die Vorschrift knüpft nicht etwa an die Beschuldigteneigenschaft der betroffenen Person an, sondern an jedwedes Ereignis (Anzeigeerstattung, Geschädigten- oder Zeugeneigenschaft etc.), das mit der betroffenen Person in Verbindung gebracht wird. Das hat zur Folge dass Daten einer Person unter Umständen jahrzehntelang gespeichert werden – ohne dass sie sich in dieser Zeitspanne etwas hat zuschulden kommen lassen.

Der Gesetzentwurf greift das Problem auf, bietet aber nur eine Teillösung an.
Denn auch die neue Formulierung hat zur Folge, dass Daten eines Beschuldigten unter Umständen Jahrzehnte gespeichert bleiben. Dies widerspricht den Grundsät-

zen der Erforderlichkeit und Datensparsamkeit. Folge einer im Einzelfall nahezu dauerhaften Speicherung kann auch das Auseinanderfallen von Aktenaufbewahrung und Datenspeicherung sein. Die Aufbewahrungsfristen für Akten sind in Bayern in der Verordnung über die Aufbewahrung von Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden (Aufbewahrungsverordnung, (GVBl. 2010, S. 644) geregelt, wonach etwa die Akten eines eingestellten Ermittlungsverfahrens grundsätzlich für die Dauer von fünf Jahren nach dem Jahr der Weglegung aufbewahrt werden. Da die Aufbewahrungsverordnung keine Mitziehung kennt, werden die Akten nach Fristablauf ausgesondert, während die entsprechenden Datensätze hierzu weiter gespeichert bleiben. Eine Überprüfung möglicherweise unrichtig gespeicherter Daten anhand der zugrundeliegenden Akten ist dann nicht mehr möglich. Weiterhin haben nach Art. 7 Abs. 2 der Richtlinie EU 2016/680 die zuständigen Behörden alle angemessenen Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig, unvollständig oder nicht mehr aktuell sind, nicht bereitgestellt werden. Zu diesem Zweck hat jede zuständige Behörde die Qualität der personenbezogenen Daten grundsätzlich vor ihrer Bereitstellung zu überprüfen. Eine Überprüfung gespeicherter Daten ist jedoch dann nicht mehr möglich, wenn die hierzu geführten Akten bereits vernichtet wurden.

Ganz aktuell hat zudem der EGMR mit Urteil vom 24.01.2019 (Az. 43514/15 – Case of Catt v. The United Kingdom) Großbritannien verurteilt, weil die britische Polizei die Daten eines 94-jährigen Friedensaktivisten unverhältnismäßig lang gespeichert hatte. In der Datei für „inländische Extremisten“ („domestic extremists“) fanden sich Speicherungen zu 66 Demonstrationen und Kundgebungen, an denen der Friedenaktivist teilgenommen hatte. Der EMGR hielt zwar die jeweiligen Einträge grundsätzlich für rechtmäßig, sah jedoch in der fortdauernden Speicherung der Daten eine Verletzung des Rechts auf Privatleben nach Art. 8 EMRK. Der EGMR monierte insbesondere das Fehlen einer zeitlichen Obergrenze für die Datenspeicherungen.

Ich empfehle deshalb,

§ 489 Abs. 5 StPO-Entwurf ersatzlos zu streichen.

Sollte der Gesetzgeber im Grundsatz an der Mitziehklausel festhalten wollen, ist zu beachten, dass die jetzt geplante Formulierung „*Werden die Daten des Beschuldig-*

ten für ein weiteres Verfahren in dem Dateisystem oder einem Informationssystem gespeichert, so kann die Löschung dieser Daten unterbleiben, bis für alle Eintragungen die Löschungsvoraussetzungen vorliegen“ zur Folge hat, dass damit die Speicherung in den staatsanwaltlichen Dateien auch von der Speicherung in polizeilichen Informationssystemen abhängig gemacht werden kann.

Für den Fall, dass der Gesetzgeber entgegen meiner Empfehlung im Grundsatz an der Mitziehklausel in § 489 Abs. 5 StPO-Entwurf festhält, rate ich dringend dazu,

die Worte „oder einem Informationssystem“ im Gesetzentwurf zu § 489 Abs. 5 StPO zu streichen.

Mit freundlichen Grüßen

gez.

Prof. Dr. Thomas Petri

Generalstaatsanwaltschaft Frankfurt am Main

Generalstaatsanwaltschaft Frankfurt am Main · 60256 Frankfurt am Main

Elektronische Post

An den
Deutschen Bundestag
- Ausschuss für Recht
und Verbraucherschutz -
Platz der Republik 1
11011 Berlin

Aktenzeichen: **10 E 7/19 SH**

Dst.-Nr.: 0223
Bearbeiter: Oberstaatsanwältin Dr. Sander
Durchwahl: 069 1367-2347
Fax: 069 1367-8352
E-Mail: lisakathrin.sander@gsta.justiz.hessen.de

Datum: 15. Februar 2019

Stellungnahme zur öffentlichen Anhörung
des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages
am 20. Februar 2019 in Berlin

zu dem „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)

Mit dem Gesetzentwurf der Bundesregierung soll das europäische Datenschutzrecht insbesondere im Strafverfahrensrecht – folglich im Anwendungsbereich der Richtlinie (EU) 2016/680 vom 27. April 2016 (nachfolgend „JI-Richtlinie“) und nicht der Verordnung (EU) 2016/679 vom 27. April 2016 (Datenschutz-Grundverordnung) – umgesetzt werden. Dementsprechend beschränke ich mich auf eine Stellungnahme zu den für die Strafverfolgungsbehörden, namentlich die Staatsanwaltschaften, maßgeblichen Änderungen.

I.

Eine wesentliche Änderung stellt bereits der Regelungsansatz des Gesetzesvorhabens an sich dar. Darin ist zur Umsetzung der JI-Richtlinie anstelle der bisherigen bereichsspezifischen Sonderregelung innerhalb der Strafprozessordnung ein weitergehender Rückgriff auf das neugefasste Bundesdatenschutzgesetz (BDSG (2018)) vorgesehen *(1.).* Bedenken in der Sache begegnet insbesondere die beabsichtigte Aufhebung der bisherigen Sonderregelung zum allgemeinen datenschutzrechtlichen Auskunftsanspruch *(2.).*

Diese aus Sicht der staatsanwaltschaftlichen Praxis maßgeblichen Einwände wurden bereits im Rahmen der Praxisbeteiligung zu dem Gesetzentwurf vorgebracht.

1. Systematischer Regelungsansatz des Gesetzentwurfs

Gegen den systematischen Regelungsansatz, wonach unter weitgehendem Absehen von einer strafverfahrensspezifischen Sonderregelung in der Strafprozessordnung ein grundsätzlicher Rückgriff auf das subsidiäre BDSG (2018) in Form der Regelungen im 3. Teil erfolgen soll (vgl. § 500 StPO-E und § 1 Abs. 2 BDSG (2018)), bestehen erhebliche praktische Bedenken. Denn infolgedessen sind Einschränkungen der Verständlichkeit und eine wesentliche Erschwerung der Rechtsanwendung zu besorgen. Es steht zu befürchten, dass entsprechenden Anwendungsschwierigkeiten durch das „neuartige Regelungsgefüge“ auch mit der weiterhin in Aussicht genommenen Ergänzung des Gesetzentwurfs durch (bislang soweit ersichtlich nicht vorliegende) „nähere Hinweise im Rahmen einer Überarbeitung der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV)“ (vgl. BT-Drs. 19/4671, S. 44) nicht begegnet werden kann.

Die Notwendigkeit einer solch grundlegenden Abkehr von der bisherigen – bewährten – Regelungstechnik im Sinne einer „kompakten“ Verfahrensordnung durch Öffnung des Strafverfahrensrechts für Regelungen außerhalb der Strafprozessordnung ist schon angesichts der damit einhergehenden Praktikabilitätseinbußen nicht zu erkennen und insbesondere nach den Vorgaben der JI-Richtlinie nicht zwingend.

Aus Sicht nicht nur der staatsanwaltschaftlichen, sondern der gesamten strafrechtlichen Anwendungspraxis erscheint – entgegen der Auffassung in der Gesetzesbegründung (vgl. BT-Drs. 19/4671, S. 71) – vielmehr eine Umsetzung der JI-Richtlinie *innerhalb* der Strafprozessordnung sinnvoll und sachgerecht. Damit ist sichergestellt, dass der Rechtsanwender die einschlägigen Normen in einem möglichst geschlossenen Gesetzeswerk vorfindet und nicht auf eine – zudem stetig unübersichtlicher werdende – Reihe unterschiedlicher Rechtsquellen zurückgreifen muss. Dies wäre auch unter systematischen Gesichtspunkten vorzugswürdig. Die Handhabbarkeit und Praktikabilität einer Verfahrensordnung stellen – gerade in einem praktisch so hoch bedeutsamen und sensiblen Bereich wie dem Strafverfahren – einen Wert an sich dar.

2. Aufhebung der bisherigen spezialgesetzlichen Sonderregelung zum allgemeinen datenschutzrechtlichen Auskunftsanspruch (§ 491 StPO-E)

Bedenken in der Sache – und zugleich exemplarisch für die Auswirkungen des soeben dargestellten Regelungsansatzes – begegnet insbesondere die vorgesehene Aufhebung der bisherigen spezialgesetzlichen Sonderregung zum allgemeinen datenschutzrechtlichen Auskunftsanspruch in § 491 StPO-E. Dazu soll die bislang in § 491 Abs. 1 Satz 1 StPO normierte teilweise Ausschlussklausel zu datenschutzrechtlichen Auskunftsansprüchen dahingehend abgeändert werden, dass das allgemeine Auskunftsrecht des BDSG (2018) Anwendung finden und nicht mehr durch andere, in der Strafprozessordnung geregelte Auskunfts- oder Akteneinsichtsrechte verdrängt werden soll (vgl. BT-Drs. 19/4671, S. 45 und 70 f.).

Das geltende Regelungskonzept einschließlich der Sperrfrist für laufende Verfahren hat sich jedoch bewährt und trägt den Belangen der Strafverfolgungsbehörden einerseits und den Interessen der Betroffenen andererseits differenziert und angemessen Rechnung. Es sollte daher – in Übereinstimmung mit der Stellungnahme des Bundesrates (vgl. auch nachfolgend BR-Drs. 433/18 (Beschluss), S. 4 f.) – beibehalten werden. Denn die Verhinderung von Gefährdungen des Untersuchungszwecks des nichtöffentlichen Ermittlungsverfahrens (vgl. auch § 353d Nr. 3 StGB betreffend Mitteilungen aus Anklageschriften) erfordert eine kohärente und zugleich *strafverfahrensspezifische* Regelung innerhalb der Strafprozessordnung.

Insbesondere die bewährte Sperrfrist für die Auskunft zu laufenden Verfahren und der Hinweis auf diese Sperrfrist bei einer Negativauskunft (§ 491 Abs. 1 Satz 2 bis 6 StPO) sollten aus Sicht der Praxis dringend beibehalten werden. Die Ausschlussfristen und der in jedem Fall zu erteilende diesbezügliche Hinweis gewährleisten einen angemessenen Ausgleich zwischen den Geheimhaltungsinteressen der Strafverfolgungsbehörden und den Belangen der Betroffenen. Die Pauschalität der Frist lässt Rückschlüsse aus einer verweigerten Auskunft nicht zu. Durch die abgestufte Fristenregelung ist zudem sichergestellt, dass die Interessen der Betroffenen auch im Einzelfall ausreichend Berücksichtigung finden.

Zugleich tragen die ausdifferenzierten Regelungen zur Akteneinsicht den Interessen der Betroffenen angemessener Rechnung als eine allgemeine Pflicht zur Durchführung einer Interessenabwägung mit weniger spezifischen Vorgaben nach dem Bundesdatenschutzgesetz (§ 491 Abs. 2 Satz 1 StPO-E i. V. m. §§ 57 Abs. 4, 56 Abs. 2 BDSG (2018)). Das im Gesetzentwurf vorgesehene „Nebeneinander des datenschutzrechtlichen Auskunftsanspruchs und der verfahrensrechtlich vorgesehenen Akteneinsichtsrechte“ (vgl. BT-Drs. 19/5554, S. 8) dürfte demgegenüber nicht zu einem inhaltlichen Mehrwert für die Auskunftsberechtigten führen, jedoch zu einer zu erwartenden Mehrbelastung durch die Bearbeitung von Auskunftsanträgen bei Staatsanwaltschaften, Führungsaufsichtsstellen und Bewährungshelfern pp.

Soweit in der Gesetzesbegründung ausgeführt wird, dass die bisherige Regelung dem „Anliegen“ der JI-Richtlinie nicht mehr gerecht werde und in einem „Spannungsverhältnis“ mit Art. 15 der Richtlinie stehe (vgl. BT-Drs. 19/4671, S. 70 f.), steht dies einer Beibehaltung der geltenden Rechtslage nicht entgegen: Denn Art. 15 Abs. 1 der JI-Richtlinie erklärt gesetzliche Einschränkungen des Auskunftsrechts der betroffenen Person (aus Art. 14) ausdrücklich für zulässig, sofern dabei „den berechtigten Interessen der betroffenen natürlichen Person Rechnung getragen wird“ (vgl. auch Art. 18 der JI-Richtlinie). Art. 15 der JI-Richtlinie verlangt demnach nicht, jede Einschränkung des Auskunftsrechts an eine Einzelfallabwägung zu knüpfen; den berechtigten Interessen der Betroffenen muss, wie zitiert, lediglich Rechnung getragen werden.

Die geltende Rechtslage mit den vorrangigen Spezialvorschriften in der Strafprozessordnung einschließlich der Sperrfrist für die Auskunft zu laufenden Verfahren ist daher – in weitergehender Übereinstimmung mit der Auffassung des Bundesrates (vgl. BR-Drs. 433/18 (Beschluss), S. 5) – auch mit der JI-Richtlinie vereinbar.

II.

Darüber hinaus ist in aller Kürze auf das vorgesehene „Datenschutzregime“ einzugehen. Angesprochen sind damit die Aufsichtskompetenzen der staatlichen Datenschutzbeauftragten, für die Landesjustiz insoweit der landesrechtlichen Aufsichtsstellen (vgl. § 500 Abs. 2 Nr. 2 StPO-E und für Hessen § 55 HDSIG). Nähere Maßgaben insbesondere zum Verhältnis des entsprechenden Beschwerderechts des Betroffenen zu den strafprozessualen Rechtsbehelfen und der fachaufsichtlichen Hierarchie der Staatsanwaltschaften sind dem Gesetzentwurf nicht zu entnehmen. Insoweit wären weitere Prüfungen im Fortgang des Gesetzgebungsverfahrens aus praktischer Sicht wünschenswert.

III.

Fazit: Eine Verfahrensordnung bedarf – erst Recht in einem so eingriffsintensiven Bereich wie dem des Strafverfahrens – größtmöglicher Handhabbarkeit und Praktikabilität. Die Belange der Anwendungspraxis finden in dem Gesetzentwurf jedoch bislang aus staatsanwaltschaftlicher Sicht nicht ausreichend Berücksichtigung. Da der Regelungsansatz nach den Vorgaben der JI-Richtlinie nicht zwingend ist und sich aus praktischer Sicht nicht empfiehlt, sollte er mit Blick auf die Verständlichkeit und Kohärenz der Strafprozessordnung dringend überdacht werden.

Mit der Ergänzung der Datenschutz-Grundverordnung um die JI-Richtlinie sollte gerade den Besonderheiten der Strafjustiz Rechnung getragen werden können. Diesen Spielraum sollte der Gesetzgeber auch gesetzestechnisch nutzen.

Dr. Sander
Oberstaatsanwältin