Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin)

Prof. Dr. Clemens Arzt
Direktor

Alt-Friedrichsfelde 60
10315 Berlin

www.foeps-berlin.org
foeps@hwr-berlin.de

Entwurf eines Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern und zur Änderung anderer Gesetze

Gesetzentwurf der Landesregierung Drs. 7/3694 vom 5. Juni 2019

Anmerkungen anlässlich der Anhörung im Innenausschusses des Landtags Mecklenburg-Vorpommern am 22. August 2019

Prof. Dr. Clemens Arzt

Fachbereich Polizei und Sicherheitsmanagement der HWR Berlin
Direktor Forschungsinstitut für Öffentliche und Private Sicherheit (FÖPS Berlin)

Berlin, den 22. August 2019
(erweiterte Fassung)

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Mit Blick auf den Gesetzentwurf der Landesregierung erlaube ich mir nachfolgende einige rechtliche Anmerkungen zu ausgewählten Regelungen. Aufgrund des Charakters dieses Papiers und insbesondere wegen des kurzen zeitlichen Vorlaufs können Fundstellen oder Urteile für meine Einschätzung hier nicht zitiert werden; diese beruhen auf meiner zwanzigjährigen Tätigkeit als Hochschullehrer für Polizeirecht und als Sachverständiger im Bundestag und vielen Landtagen. Ich möchte auch darauf hinweisen, dass nachfolgende Anmerkungen sich nicht auf den vorgenannten Entwurf alleine beziehen, sondern zum Teil auch bereits vorhandene Normen im SOG M-V einbezogen werden, weil anders eine sinnvolle Analyse des neuen Gesetzes als Ganzem nicht möglich erscheint.

Zum Gesetzentwurf erlaube ich mir in diesem Rahmen nachfolgende Anmerkungen:

1. Der GE reiht sich ein in eine **Kette von Verschärfungen des Polizeirechts in Deutschland**, die seit dem 11. September 2001 und seit dem Anschlag auf dem Berliner Breitscheidplatz offenbar staatliche Handlungsfähigkeit demonstrieren sollen, ohne auch nur im Ansatz evidenzbasiert darzulegen, wo Lücken im bestehenden Rechts bestehen (sollen). Es wird einfach auf den „Terrorismus“ und die allgemeine Kriminalitätsentwicklung verwiesen und das muss zur Begründung ausreichen. Hier kommt der Eindruck von **symbolischer Gesetzgebung** auf, anstelle einer Schwachstellenanalyse im geltenden Recht, mit konkretem Bezug auf die tatsächliche Lage in M-V.

2. Konterkariert wird damit zudem das im GE kurz erwähnte Vorhaben einen neuen **Musterentwurfs für ein einheitliches Polizeigesetz** in Deutschland, weil seit 2017/18 angefangen mit Baden-Württemberg und Bayern eine Vielzahl von Bundesländern das Polizeirecht im Sinne breiter Befugniserweiterungen und neuer Befugnisse zu Lasten der Freiheitsrechte der Bürger*innen erweitert hat, die anzupassen an einen ME im Nachgang kaum noch gelingen wird, weil jedes

Bundesland dabei spezifische eigene Ansätze umsetzt, die im Nachgang zu vereinheitlichen mE nicht mehr gelingen wird.

3. Bei aller Kritik im Folgenden soll positiv hervorgehoben werden, dass wesentliche Teile des **polizeirelevanten Datenschutzrechts**, dessen Novelle aus europarechtlichen Pflichten (**DSGVO und RL 2016/608** = JI-RL) seit Mai 2018 überfällig ist, im SOG M-V in einem Gesetz zusammengefasst und mit Blick auf die direkte Anwendbarkeit der DSGVO auch abgegrenzt werden. Dabei bleiben allerdings weiterhin zusätzliche Regelungen im DSG M-V bestehen, was die Übersichtlichkeit erschwert.

   Diese Anpassungen sind im Kern notwendig mit Blick auf die ohnehin bereits um mehr als eineinhalb Jahre **europarechtswidrig verspätete Umsetzung** der JI-RL. Allerdings beschränkt sich der GE häufig auf eine bloße Wiederholung der JI-RL, was nicht selten verzichtbar wäre, weil die RL die Umsetzung eben dem nationalen Gesetzgeber überlässt und keinesfalls erzwingt, jedwede Regelung dort durch vollgegenständliche Wiederholung in das nationale Recht zu inkorporieren.

   Auch eine **bloße Übernahme von Vorschriften der §§ 45 ff. BDSG** ist nicht zielführend und verkürzt die parlamentarische Betrachtung. Zudem verbleibt diese sehr häufig auf einer sehr abstrakten Ebene, statt zum Beispiel Anforderungen an den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen im Sinne des Art. 20 JI-RL (*privacy by design* und *privacy by default*) oder auch eine datenschutzrechtliche Folgenabschätzung mit Bezug auf die (neuen) Maßnahmen im SOG auch in konkrete Anforderungen umzusetzen. Dies wäre dann ein wirklich dem Datenschutz verbundenes Gesetzgebungsprojekt.

4. Ich werde mich daher im Folgenden nicht explizit auf die neuen Maßnahmen aus diesem GE allein beschränken, weil nur eine **Gesamtschau** des Potpourri immer neuer Maßnahmen eine sachgerechte Beurteilung und Einordnung erlaubt. Zum

Teil gravierende Beschränkungen von Grundrechten beinhalten insbesondere folgende Maßnahmen:

a. Bild- und Tonaufnahmen im öffentlichen Raum einschließlich Übersichtsaufnahmen und –aufzeichnungen
b. Bild- und Tonaufnahmen in Gewahrsamseinrichtungen
c. Bild- und Tonaufnahmen zur Suche nach gefährdeten Personen
d. Bodycam
e. Online Durchsuchung
f. Vielfältige Eingriffe in das Telekommunikationsgrundrecht und das Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme
g. Drohneneinsatz
h. Ausschreibung zur Beobachtung und gezielten Kontrolle
i. Erweiterung des Katalogs erheblicher Straftaten
j. Einführung eines Katalogs terroristischer Straftaten
k. Erweiterung von Befugnissen zur „Verhütung terroristischer Straftaten“
l. Meldeauflagen
m. Einführung des gezielten Todesschusses
n. Beschränkung der Versammlungsfreiheit durch Polizeirecht

Der GE enthält damit eine erhebliche Anzahl umstrittener und rechtlich problematischer neuer Maßnahmen oder deren Ergänzung, Erweiterung oder auch nur Anpassung an europarechtliche Regelungen zum Datenschutz, namentlich die DSGVO und die JI-RL. Die vorgenannten Maßnahmen (der Katalog ist dabei keinesfalls als abschließend zu betrachten), die auch nur einen Teil des GE umfassen, können aus Zeitgründen hier nur in Teilen kurz kommentiert werden, wobei ich in der Öffentlichkeit besonders umstrittene Maßnahmen wie zB die **Onlinedurchsuchung, die (Quellen-)TKÜ, die Rasterfahndung und Meldeauflagen** nicht oder nur sehr kurz kommentiere, weil hier davon auszugehen ist, dass in der öffentlichen Anhörung am 22.8.2019 sich eine Reihe

anderer Sachverständiger hierzu äußern wird. Auf die Stellungnahme zur öffentlichen Anhörung am 22. August 2019 im Innenausschuss des LT von Prof. Dr. Roggan darf ich insoweit ausdrücklich verweisen.

5. Auch wenn die **Umsetzung wesentlicher Teile des EU-Datenschutzrechts** im SOG selbst diesseits grundsätzlich als sinnvoll angesehen wird – und bei entsprechendem zeitlichem Vorlauf näher zu analysieren wäre – ist doch anzumerken, dass eine klare Abgrenzung von der DSGVO einerseits und der JI-RL andererseits unterfallenden Aufgaben der Polizei nicht gänzlich gelungen scheint. Hinzu kommt, dass neben dem SOG weitere Regelungen zur Umsetzung der JI-RL sich im DSG M-V befinden, was für die handelnden Polizeivollzugsbeamt*innen durchaus Fragen zur Anwendbarkeit des Rechts aufwerfen wird. Eine Inkorporierung der einschlägigen Regelungen des DSG M-V in das SOG M-V erschiene daher als besserer Weg. Im Übrigen sei kurz angemerkt:

   a. Zum einen wäre es aus meiner Sicht unbedingt sinnvoll und auch mit Blick auf die grundrechtliche Notwendigkeit einer strikten Unterscheidung und expliziten Regelung jedes „Verarbeitungsschrittes“ notwendig, anstelle des breiten EU-rechtlich geprägten Begriffs der Datenverarbeitung weiterhin im Gesetz an jeder Stelle alle zulässigen „Etappen“ der Datenverarbeitung im Sinne der herkömmlichen Terminologie von Erhebung, Speicherung, Nutzung, Veränderung, Löschung, Übermittlung etc. zu bezeichnen. Diese geschieht zwar an vielen Stellen, zum Beispiel mit Blick auf die vielfältigen Varianten von Bild- und Tonaufnahmen aber nicht immer.

      Hier sei als Beispiel nur auf § 32a I 1 verwiesen, nach dem die Polizei mittels Bodycam Bild- und Tonaufnahmen „im Zwischenspeicher erheben“ kann. Gemeint ist offenkundig eine Erhebung und anschließende Speicherung, was zwei getrennt zu beurteilende

Grundrechtseingriffe darstellt, aber durch den Wortlaut „überdeckt“ und nicht mit der hinreichenden Normenklarheit geregelt wird.

b. Zum anderen – und hierauf kann nur kurz hingewiesen werden, würde aber eine umfassende Analyse rechtfertigen – werden im GE (S. 152) bestimmte polizeiliche Aufgabenbereiche, wie der des Schutzes privater Rechte der JI-RL zugewiesen, obgleich der Schutz PRIVATER Rechte in § 1 III gerade als gesonderter Aufgabenbereich jenseits der Gefahrenabwehr benannt ist und hierfür auch nur eng begrenzte Befugnis des SOG in Betracht kommen. Maßnahmen (allein) in diesem Aufgabenbereich unterfallen daher der DSGVO und nicht der JI-RL.

6. Nach **§ 4 I 2** [Angaben zu §§ beziehen sich stets auf das SOG M-V, soweit nicht anders angegeben], soll künftig die Gefahrenabwehr auch die „**Verhütung von Ordnungswidrigkeiten**“ umfassen. Dies ergibt sich bereits aus der allgemeinen Definition der (konkreten) Gefahr und wäre insoweit verzichtbar. Dahinter steht aber in Folge mit Blick auf die gesetzlichen Neuregelungen eine deutliche Ausweitung polizeilicher Eingriffsbefugnisse, die bisher allein der „Verhütung von Straftaten“ vorbehalten war, beispielsweise hinsichtlich der Zweckänderung nach § 36 I, II (die immerhin eine gesetzliche Durchbrechung der grundrechtlich vom BVerfG jüngst in der Entscheidung zum BKAG bestätigten Zweckbindung darstellt) oder auch der **Übermittlung** von Daten zur Verhütung von Ordnungswidrigkeiten an Nicht-EU-Mitgliedsstaaten (**Drittstaaten**).

   Noch gravierender ist hier sicherlich die die Zulässigkeit einer **Zweckänderung von zur Protokollierung von Datenverarbeitungsvorgängen gespeicherten Protokolldaten**, die zukünftig nach **§ 46e IV** sogar zur Verhütung von Ordnungswidrigkeiten sollen genutzt werden können. Bisher waren vergleichbare Zweckänderungen in anderen Gesetzen auf die Abwehr gegenwärtiger Gefahren für Leib oder Leben und vergleichbare Tatbestände begrenzt. Hier bedarf es nicht einmal der konkreten Gefahr einer Begehung solcher Ordnungswidrigkeiten.

7. Die Regelung zur **sachlichen Zuständigkeit der Polizei** beruht mit Blick auf § 7 I Nr. 4 auf einem seit fast 15 Jahre **obsoleten Konzept der Vorsorge für die Verfolgung von Straftaten (Verfolgungsvorsorge)** als Teil der Gefahrenabwehr, beruhend übrigens auf einer Formulierung im Musterentwurf für ein einheitliches Polizeigesetz (VE zur Änderung des MEPolG vom 12. März 1986). Nun hat aber das BVerfG in seiner Entscheidung zur Verfassungswidrigkeit der Telekommunikationsüberwachung (TKÜ) nach dem NdsSOG bereits 2005 festgestellt, dass **Verfolgungsvorsorge repressiv-polizeiliches Recht** darstellt, also Strafprozessrecht. Einige Bundesländer und das BPolG haben hieraus die Konsequenz gezogen, diesen Aufgabenbereich aus ihren Gesetzen zu streichen. Das hat das BVerfG so nicht unbedingt gefordert, wohl aber eine klare Abgrenzung des Landesgesetzgebers für jede Maßnahme der Verfolgungsvorsorge von eventuellen Maßnahmen in der StPO und sogar dem in den Gesetzgebungsmaterialien eventuell erkennbaren Verzicht auf bestimmte Maßnahmen.

   Zumindest in dem hier zu beurteilenden Gesetzgebungsverfahren ist eine solche **Prüfung anhand der Maßstäbe des BVerfG nicht erkennbar** und nicht wenige Maßnahmen sind aus meiner Sicht mit dieser Rechtsprechung nicht vereinbar oder müssten zumindest auf ihre Verfassungskonformität am Maßstab des BVerfG aus 2005 überprüft werden, wofür in jedem Einzelfall zu prüfen wäre, ob nicht der Bund im Rahmen der StPO bereits Regelungen erlassen oder deutlich gemacht hat, dass solche Maßnahmen nicht erlassen werden sollen.

   Dabei wäre auch zu fragen, ob ein „**Verstecken**“ vielfältiger Maßnahmen im Bereich des repressiv-polizeilichen **Rechts der Verfolgungsvorsorge im Polizeirecht** mit den Anforderungen an die Normenklarheit und Transparenz im Eingriffsrecht vereinbar ist.

8. § 25a IV gestattet die **ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung**, einschließlich Profiling, wenn diese durch das SOG

zugelassen ist und nicht auf besonderen Kategorien personenbezogener Daten beruht. Auch wenn eine solche Maßnahme bisher im SOG nicht vorgesehen ist, schafft der Gesetzgeber hier die Grundlagen für solche Maßnahmen, wozu er durch die JI-RL nicht verpflichtet ist, solange er eine solche Maßnahme nicht nutzt. Im Sinne der Freiheitsrechte der Bürger wäre hingegen, einen völligen Verzicht auf solche Maßnahmen im SOG festzuschreiben, wenn hier nicht schon vorsorglich eine Grundlage für die zukünftige Einführung geschaffen werden soll.

9. **§ 25b** regelt gerichtliche Zuständigkeit für **richterliche Entscheidungen**, von denen das Gesetz auch einige neu einführt. Hier ist zum einen grundsätzlich zu fragen, ob diese richterlichen Entscheidungen vorab den **Amtsgerichten** zugeordnet werden soll, während deren Rechtmäßigkeit im Nachhinein in vielen Fällen den Verwaltungsgerichten zugewiesen ist. Letzteren gehörten richterliche Entscheidungen im Polizeirecht als Teil des öffentlichen Rechts nach der hier vertretenen Auffassung hingegen sinnvoller Weise zugeordnet, weil am AG nicht selten die/der Bereitschaftsrichter*in entscheidet, die sonst Aufgaben aus anderen Rechtsgebieten als denen des öffentlichen Rechts wahrnehmen. Auch die Zuordnung von Entscheidungen zur Gewahrsamnahme oder Wohnungsdurchsuchung, die auch die StPO kennt, kann mE eine solche Zuordnung nicht sinnvoll begründen. Diese Frage sollte daher in Zukunft geprüft werden, auch wenn dies im Rahmen dieses Verfahrens sicherlich nicht hinreichend zu diskutieren sein wird.

10. Etwas Anderes ist der ebenfalls in § 25b nicht hinreichend bestimmte **Verweis auf das Gesetz über das Verfahren in Familiensachen und Angelegenheiten der freiwilligen Gerichtsbarkeit** (FamFG), das für alle Entscheidungen nach dem SOG zur Anwendung kommen soll. Dieser Hinweis ist im Gesetz selbst hinreichend zu spezifizieren, also zB auf das Siebte Buch für freiheitsentziehende Maßnahmen und ggf. auf andere Regelungen für andere Entscheidungen, die durch das SOG neu den Amtsgerichten zugewiesen werden.

Ein **Mangel an Normenbestimmtheit** durch Abwesenheit solcher klaren Festlegungen führt dazu, dass für Betroffene, Polizei und auch Gerichte nicht hinreichend klar ist, welche Verfahrensvorschriften überhaupt zum Beispiel bei einer elektronischen Aufenthaltsüberwachung oder einer Online-Durchsuchung anzuwenden sein sollen; dies dürfte mit der in Art. 19 IV GG garantierten **Rechtsschutzgarantie** schwerlich vereinbar sein. Hier muss der Landesgesetzgeber selbst eine klare Entscheidung treffen, welche Regelungen aus dem Bundesrecht anwendbar sein sollen.

11. **§ 26** regelt ausführlich die **Einwilligung des Betroffenen** in eine Verarbeitung personenbezogener Daten. Dabei wird verkannt, dass im Verhältnis von Bürger und Polizei es eine Freiwilligkeit der Einwilligung nicht geben kann, wenn der Staat das Verlangte auch durch polizeiliche Maßnahme erreichen könnte. Es sollte daher klargestellt werden, dass eine Einwilligung nur in Betracht kommt, wo Bürger*innen von sich aus personenbezogene Daten der Polizei zur Verfügung stellen.

12. **§ 27 III** regelt die **Erhebung personenbezogener Daten mit Blick auf mögliche terroristische Straftaten** im Sinne von § 67c (dessen Katalog extrem weit ist und trotz nachhaltiger Kritik in der Strafrechtswissenschaft auch Handlungen umfasst, die bisher zu keiner Rechtsgutverletzung geführt haben, wie etwa §§ 89a bis c StGB oder auch Delikte umfasst wie Computersabotage oder die Zerstörung fremder technischer Arbeitsmittel). Zur Datenerhebung sollen hier tatsächliche Anhaltspunkte für die künftige Begehung solcher Straftaten genügen. Problematisch ist insbesondere, dass das Gesetz hier - anders als etwa in Absatz 1 - an keiner Stelle näher spezifiziert, zu **welchem Zwecke** diese Daten erhoben werden dürfen. Sollen diese der Gefahrenabwehr, der Verhütung von Straftaten oder der Verfolgungsvorsorge dienen dürfen – oder allen drei Aufgaben zugleich?

Dies **widerspricht** dem **Bestimmtheitsgebot**, an das im Bereich so extensiver Befugnisse zur Erhebung personenbezogener Daten hohe Anforderungen zu stellen sind, zumal hier nach Absatz 4 auch **besondere Kategorien personenbezogener Daten** (zB zur Ethnie, politischen Meinung, Religion, genetische Daten, Daten zur sexuellen Orientierung und mehr) erhoben werden dürfen.

Anders als Absatz 3 wird zudem in Satz 1 die Maßnahme auf die Abwehr (konkreter) Gefahren begrenzt, was wiederum im Widerspruch dazu steht, das im gleichen Satz auf Absatz 3 Nr. 1 und 2 verwiesen wird, die gerade keine konkrete Gefahr verlangen. **Die Norm ist also widersprüchlich in sich selbst** und verstößt damit gegen das **Gebot der Bestimmtheit** tatbestandlicher Voraussetzungen für einen solchermaßen schweren Grundrechtseingriff.

13. **§ 27a** I gestattet umfangreiche so genannte **Anhalte- und Sichtkontrollen**. **Absatz 1 Nr. 1** räumt dabei der Polizei weitgehende Befugnisse zu im Gesetz genannten Zwecken ein, **ohne** hierfür überhaupt irgend geartete **tatbestandliche Anforderungen** festzulegen. Das Gebot der **Normenbestimmtheit** verlangt anderes.

    Die Regelung ist in **Absatz 1 Nr. 2** zudem im Konflikt mit den durch das Schengener Grenzabkommen ausgeschlossenen „**verkappten Grenzkontrollen**“, die seit einiger Zeit zunehmend von den Gerichten (insbesondere mit Blick auf das BPolG) beanstandet werden. Eine Auseinandersetzung mit dieser Rechtsprechung ist im GE indes an keiner Stelle erkennbar. Auch diese Regelung dürfte im Anfechtungsfalle einer verwaltungsgerichtlichen Kontrolle kaum standhalten.

    Wie die in diesem Kontext erlaubte **Augenscheinnahme** von Fahrzeugen im Polizeialltag klar von einer Durchsuchung abgegrenzt werden soll, ist fraglich.

14. Mit Blick auf die **Befragung in § 28 II** soll hier – obgleich es sich nicht um eine Neuregelung handelt – angemerkt werden, dass insbesondere die

Auskunftspflicht für Personen die nicht unter §§ 69, 70 fallen, rechtlich problematisch ist, weil diesen – noch dazu ohne weitere Tatbestandsvoraussetzungen – nach der hier vertretenen Auffassung **keine Auskunftspflicht** auferlegt werden kann. Es gibt keine Pflicht der Bürger*innen zur „Kooperation“ mit der Polizei.

Gerade mit Blick auf Verantwortliche nach den vorgenannten Normen ist aber auch der *nemo-tenetur*-Grundsatz, also der **Grundsatz der Selbstbelastungsfreiheit** aus § 136 I 2 StPO zu beachten, auf den interessanterweise in Absatz 2 gerade nicht verwiesen wird. Wird eine Gefahr im klassischen polizeirechtlichen Sinne hervorgerufen, beruht dies häufig gerade auf der Verletzung einer Straf- oder Ordnungswidrigkeitennorm und die **Pflicht zur Aussage** kommt schnell mit dem vorgenannten Grundsatz **in Konflikt**.

15. Durch **§ 29 I Nr. 4** werden die nicht durch eine Handlung des Kontrollierten begründeten Befugnisse der Polizei zu **Identitätsfeststellungen** erheblich ausgeweitet. Jede solche Kontrolle stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar und bedarf daher der besonderen Rechtfertigung.

    Nr. 4 gilt für **Kontrollstellen** zur **Verhütung von Straftaten** und knüpft in keiner Weise am Handeln oder der Verantwortlichkeit des Betroffenen an, sondern allein daran, an einer Kontrollstelle angetroffen zu werden (also gleichsam eine „Ortshaftung“ wie auch zB Nr. 1). Es soll genügen, dass an irgendeinem Ort im Lande „tatsächliche Anhaltspunkte“ für die Begehung der sodann in Buchstabe a) bis e) aufgeführten Straftaten aus Sicht der Polizei vorliegen.

    Bedenklich ist dabei insbesondere die **weitere Ausweitung des Katalogs terroristischer Straftaten** jenseits der Katalogstraftaten des § 129a StGB um die in § 67c genannten Straftaten.

    Hinsichtlich der ebenfalls genannten Straftaten nach **§ 27 Versammlungsgesetz** ist anzumerken, dass nicht erkennbar ist, wie eine Identitätsfeststellung zum Auffinden der dort genannten Gegenstände wie Waffen, Schutzgegenständen

und Vermummung führen sollte; hierzu ist die Maßnahme **schlicht ungeeignet**. Zudem ist in diesem Kontext auf Art. 8 GG zu verweisen, das **Versammlungsgrundrecht**. Obgleich diese Befugnis auch schon in der geltenden Fassung des SOG enthalten war, wurde dort **Art. 8 GG bisher nicht zitiert**; ein **Verstoß gegen das Zitiergebot aus Art. 19 I GG**, der zur Verfassungswidrigkeit der Norm führt. In der Begründung wird auf diese Änderung und die nunmehr vorgesehene Einfügung des Art. 8 GG in die Aufzählung der eingeschränkten Grundrechte mit keinem Wort eingegangen; das ist bemerkenswert mit Blick auf die Verfassungswidrigkeit der seit Jahren bestehenden Regelung. Insoweit wäre die Behebung dieses Defizits natürlich zu begrüßen.

Allerdings sollte mit Sicht auf die polizeiliche Praxis überdacht werden, dass die bessere **Alternative** eine **Streichung des § 29 I Nr. 4 lit. e**) wäre. Wird nämlich die Polizei nunmehr ermächtigt, im Schutzbereich des Art. 8 GG nicht nur Maßnahmen nach dem Versammlungsgesetz zu treffen, sondern in unmittelbarem Kontext auch auf das SOG zurück zu greifen, kann dies bei den Beamt*innen den Eindruck erwecken, dass der Grundsatz der **Polizei(rechts-)festigkeit** aufgegeben wurde und nunmehr auch andere **Maßnahmen nach dem SOG** im **Schutzbereich des Versammlungsgrundrechts** zur Anwendung kommen. Wollte man – entgegen der Einwände zur Geeignetheit der Norm – auf die Maßnahme nicht verzichten, sollte diese in einem noch zu schaffenden und nur für Versammlungen iSd Art. 8 GG geltenden Landesversammlungsrecht verankert werden.

16. Soweit **§ 32 I die offene Datenerhebung** gestattet, ist zu hinterfragen, wie diese bei einem Einsatz von **Drohnen nach § 34** gewährleistet werden kann; die in der Gesetzesbegründung bspw. erwähnte Ausstattung des Drohnenpiloten mit einer entsprechend beschrifteten Weste wird kaum ernsthaft gerade im Anwendungsfall des Absatz 1 Nr. 2 zur Anwendung kommen können.

    In **§ 32 II** ist zudem nicht erkennbar, was genau die **Tatbestandsvoraussetzungen** der Norm sein soll: Handelt es sich um eine Maßnahme der Abwehr konkreter

Gefahren oder um eine solche zur Verhütung von Straftaten oder Ordnungswidrigkeiten; die Regelung ist mit dem Gebot der **Normenbestimmtheit nicht vereinbar.** Auch die Zielrichtung der Maßnahme ist nicht klar.

Die beiden vorgenannten Regelungen wie auch die in Absatz 3 dienen wohl realiter vor allem der **Vorsorge für die Verfolgung von Straftaten**, also der vorgezogenen Repression für den Fall der Begehung von Straftaten; mit den oben bereits beschriebenen kompetenzrechtlichen Problemen.

Unklar ist auch, wann aus Sicht des Gesetzgebers eine **„offenkundige" Datenverarbeitung** vorliegen soll; auch hier besteht ein Problem der **Normenbestimmtheit**. Aber auch faktisch sind hier Problemlagen mit Blick auf die offene Durchführung der Maßnahme greifbar, insbesondere bei Rückgriff auf **Drohnen** iSv § 34.

Niemals offenkundig ist zudem, **welche Maßnahme** die Polizei gerade durchführt: Bildaufnahmen, Bild- und Tonaufnahmen, Aufzeichnungen derselben, Übersichtsaufnahmen, Übersichtaufzeichnungen. Sollen hier kurzfristig zu wiederholende Lautsprecheransagen erfolgen – und welche Wirkung haben diese mit Blick auf mögliche Einschüchterungswirkung? Dies sind Fragen, denen sich die Rechtsprechung zur Videoüberwachung von Versammlungen seit Jahren intensiv widmet; eine kritische Reflektion dieser Rechtsprechung im Gesetzgebungsverfahren ist nicht erkennbar.

Es ist für die Betroffenen in aller Regel **nicht erkennbar**, welche Maßnahme nach § 32 die Polizei gerade durchführt und ob diese sich auf die **Datenerhebung** beschränkt oder auch eine **Datenspeicherung** durchführt. Insoweit kann der Ausnahmetatbestand der jederzeitigen Erkennbarkeit qua „Offenkundigkeit" verfassungsrechtlich keinen Bestand haben, mangels Erkennbarkeit der faktischen Maßnahme, womit für die Betroffenen auch keinerlei Möglichkeit besteht, die Rechtmäßigkeit der Maßnahme zu überprüfen.

Zu all diesen Fragen fehlen Maßgaben zu ***privacy by design*** und **privacy by default** (Art. 20 JI-RL). Wie ist sicherzustellen, dass Kameras für

Übersichtsaufnahmen keine Aufzeichnungen fertigen dürfen? Was macht ein eingesetztes System der Videoüberwachung zu einem für „**Übersichts"aufzeichnungen**, wenn doch zugleich eine **Identifizierung** der erfassten Personen zulässig sein soll? Worin liegt hier die technische Unterscheidung zu sonstigen von Absatz 1 Nr. 2 erfassten Bild- und Tonaufzeichnungen? Viele weitere Fragen drängen sich auf, die doch spätestens bei der **Anpassung an das EU-Datenschutzrecht** und namentlich Art. 20 der JI-RL im Rahmen der jetzigen Novelle eine gesetzgeberische Antwort verlangen.

17. Hinsichtlich der **Bild- und Tonaufzeichnungen in Gewahrsamsräumen nach § 32 IX** erstaunt zunächst, dass die Gesetzesbegründung nicht etwa auf den Schutz der Betroffenen im Gewahrsam abstellt, sondern den der dort tätigen Polizeibeamt*innen. Die verfehlt das Problem einer mangelnden Aufklärbarkeit möglicher polizeilicher Übergriff im geschützten Rahmen des Gewahrsams.
    Mit Blick auf die **Anforderungen** aus Art. 20 JI-RL zu ***privacy by design*** und ***privacy by default*** fehlt in der Regelung zudem jedwede Vorgabe zur Durchführung der Maßnahme. Anstatt diese Anforderungen nur allgemein irgendwo im Gesetz zu wiederholen, wäre hier eine Umsetzung der Anforderungen *in concreto* notwendig. Gesetzlichen Regelungen zum **Schutz der Privatsphäre der Betroffenen** (zB im Bereich von Toiletten) fehlen vollständig.
    Anstelle einer Löschung nach spätestens zwei Wochen (Absatz 7 Satz 2) wäre zudem zu regeln, dass die Daten **unverzüglich nach Freilassung zu sperren** sind und sodann zumindest für einen Monat für den Fall der Geltendmachung von Ansprüchen gegen die Polizei gespeichert werden, um bspw. die im Verwaltungsrecht übliche Monatsfrist als Maßstab heranzuziehen, wofür allerdings auch eine Belehrung des Betroffenen über seine Rechte notwendig wäre.

18. Mit Blick auf **§ 32 X**, der **Bild- und Tonaufnahmen zur Suche nach Personen**, deren Leben oder Gesundheit gefährdet ist gestattet, ist unklar, an welchen

Anwendungsbereich hier gedacht wird. Soll hier ernsthaft ein Bereich des öffentlichen Raumes mit allen sich dort bewegenden Personen überwacht werden – ohne das hier der in Bezug genommene Absatz 6 eine Begrenzungsfunktion haben könnte und wie soll auf eine solche Maßnahme hingewiesen werden? Sogar die Löschung wird unter schlichtem Verweis auf eine zulässige Weiterverarbeitung unter Vorbehalt gestellt. Mit Blick auf das Übermaßverbot erscheint diese Regelung zumindest unterkomplex.

19. Mit Blick auf die **Bodycam** ist zu **§ 32a** anzumerken, dass sich noch kein Gesetzgeber in Deutschland jemals der Mühe unterzogen hätte, die seit Jahren im Einsatz befindlichen und vergleichbaren Fahrzeugkameras der Polizei auf ihre Wirksamkeit hin zu evaluieren. Auch hier zeigt sich, **evidenzbasierte Gesetzgebung** ist im Bereich der inneren Sicherheit kein relevantes Paradigma legislatorischen Handelns.

    Aus rechtsdogmatischer Sicht sei darauf hingewiesen, dass die Regelung auf der Rechtsfolgenseite widersprüchlich und inkonsistent ist. Wenn die Polizei nach § 32a I 1 die Befugnis haben soll, personenbezogene Daten „**im Zwischenspeicher [zu] erheben**“, ist dies mit üblichen datenschutzrechtlichen und auch technischen Begrifflichkeiten nicht in Einklang zu bringen, weil eben eine **Erhebung keinen Speicher** braucht, sondern erst die Speicherung, was auch die eingangs genutzte Begrifflichkeit der Bild- und Tonaufzeichnung bestätigt. Erlaubt wird hier also das ***Prerecording***, obgleich die Voraussetzungen des Absatz 2 noch nicht vorliegen.

    Ob als Tatbestandsvoraussetzung die allgemeine Berufs- und Lebenserfahrung bereits die tatbestandlichen Anforderungen erfüllt oder nicht, ist nach dem Wortlaut der Norm nicht klar, weil nicht „im Einzelfall“ mit „hinreichender Wahrscheinlichkeit“ ein sodann näher qualifiziertes Ereignis gefordert wird, sondern nur die hinreichende Wahrscheinlichkeit eines Übergriffs bei der präventiv- oder repressiv-polizeilichen Aufgabenwahrnehmung. Dies sollte klargestellt werden.

Auch bei der Nutzung der Bodycam stellen sich Fragen hinsichtlich der **Offenheit** der Durchführung der Maßnahme. **Unklar** ist bereits, wer zulässigerweise Adressat der Maßnahme sein kann und ob und inwieweit sich diese auch auf Dritte beziehen kann. Auch hier fehlen Maßgaben zu ***privacy by design*** und ***privacy by default*** (Art. 20 JI-RL). Wie weit soll etwa der Aufnahmebereich der eingesetzten Kameras reichen, wie weit deren akustische Aufnahmekapazität? Dürfen Dritte erfasst werden?

20. Zu den **besonderen Mitteln der Datenerhebung in § 33** ist in Absatz 2 Satz 3 geregelt, dass diese auch zur Anwendung kommen können, „wenn die Aufklärung des Sachverhaltes zum Zwecke der Verhütung **terroristischer Straftaten** oder **ihrer möglichen Verfolgung** ansonsten unmöglich oder wesentlich erschwert wäre." Hier wird also eine Nutzung dieser Mittel mit dem bewussten Ziel entweder der **Verfolgungsvorsorge** oder bereits der **Beweissicherung** für die Strafverfolgung erlaubt. Letzteres wäre im Polizeirecht schlichtweg unzulässig; ersteres allenfalls nach hinreichender Abgrenzung zu den strafprozessualen Mitteln in der StPO (zur Problematik der Verfolgungsvorsorge ausführlicher bereits oben). Die Regelung ist daher aus kompetenzrechtlicher Sicht mehr als problematisch und es fragt sich, ob hier nicht eine verdeckte Maßnahme zur **Verdachtsgewinnung** erlaubt wird.

21. Der **Ausschreibung zur gezielten Kontrolle** gemäß **§ 35 II** zur Verhütung u.a. von so genannten terroristischen Straftaten nach § 67c ist ausgesprochen problematisch, soweit hier auch gestattet wird, die **Identität aller in einem ausgeschriebenen Fahrzeug angetroffenen Personen** festzustellen, weil es diesen an jeder weiteren „Qualifikation" im Sinne einer relevanten Kontakt- und Begleitperson fehlt. Hier wird Jede*r einer IDF allein deshalb unterworfen, weil er oder sie unter Umständen zufällig (zum Beispiel im Rahmen des Car Sharing oder einer Mitfahrgelegenheit oder auch privaten Beziehung) sich ohne Kenntnis der Umstände in einem **ausgeschriebenen Fahrzeug** befindet, das nicht einmal

von einer Person iSv Absatz 1 Satz 1 gesteuert werden muss. Dies **verletzt das verfassungsrechtliche Übermaßverbot**.

22. Mit Blick auf die **Durchbrechung der Zweckbindung** in **§ 36 I** ist fraglich, ob in Absatz 1 die gewählte Formulierung „derselben Aufgaben …“ den Anforderungen des BVerfG im Urteil zum BKAG (Rn. 278 ff.) entspricht, weil hier nicht mehr als eine Bindung an abstrakt durch die Aufgabennorm bestimmte Aufgaben besteht. Wenn hiermit jedwedes Aufgabenfeld im Rahmen des § 1 gemeint ist, führt dies zu einer **Zweckänderung ohne wirksame gesetzliche Begrenzung der Zulässigkeit**, was nach der hier vertretenen Auffassung jenseits des vom BVerfG in der vorgenannten Entscheidung (siehe auch GE Seite 193 unten) zulässigen weiteren Verwendung liegt.

    Soweit in § 36 II Nr. 2 auf im Einzelfall **konkrete Ermittlungsansätze „zur Verfolgung“ von Straftaten** abgestellt wird, ist fraglich, ob hiermit nicht bereits eine **repressiv-polizeiliche Nutzung durch das Polizeigesetz** gestattet werden soll, was kompetenzrechtlich mit Blick auf die Gesetzgebungskompetenz des Bundes für das Strafprozessrecht unzulässig wäre.

    Im Anschluss hieran gestattet § 36 IV sodann sogar eine **Identifizierung** einer Person (auch) **zur Strafverfolgung**, noch dazu unter Nutzung besonderer Kategorien personenbezogener Daten; ebenfalls eine kompetenzrechtliche Gradwanderung.

23. **§ 38** regelt die Verwendung von personenbezogenen Daten zur **Vorgangsverwaltung**. Trotz der positiv hervorzuhebenden Zweckbindung in Satz 1 letzter Halbsatz mangelt es der Norm an hinreichenden Festlegungen zur Transparenz der Datenverarbeitung und damit einem hinreichenden Schutz des Rechts auf informationelle Selbstbestimmung. Wenn in Satz 3 alle weiteren Festlegungen zu Mitteln und Umfang der Vorgangsverwaltung durch **Verwaltungsvorschrift** bestimmt werden sollen, haben die hiervon Betroffenen keine Möglichkeit, deren Vereinbarkeit mit den Anforderungen des nationalen

und europäischen Datenschutzrechts zu hinterfragen. Aus rechtsstaatlicher Sicht wie auch mit Blick auf das Vertrauen in die Rechtmäßigkeit der Verwaltung sollten solche Regelungen – die ja einen allein abstrakten Charakter haben und gerade nicht der polizeilichen Arbeit im Einzelfall dienen – daher in einer Rechtsverordnung geregelt werden oder zumindest die Veröffentlichung der Verwaltungsvorschrift im Amtsblatt vorgegeben werden.

24. Nach **§ 41 Nr. 2** soll die Polizei personenbezogene Daten zum Zwecke der Ermittlung der Identität oder des Aufenthaltes oder zur Warnung öffentlich bekannt machen, wenn die Verhütung oder Vorsorge für die Verfolgung dieser Straftat auf andere Weise nicht möglich ist. Es soll also unter sehr niedrigen Tatbestandsvoraussetzungen gleichsam eine **präventive Öffentlichkeitsfahndung** zur **Vorsorge für die Verfolgung noch nicht begangenen Straftaten** erlaubt werden. Eine Abgrenzung zu § 131b StPO erfolgt hier im GE ebenso wenig, wie eine Prüfung mit Blick auf die vorgenannte Rechtsprechung des BVerfG von 2005. Die Maßnahme dürfte die Grenzen der Zulässigkeit repressiv-polizeilicher Maßnahmen im Polizeirecht überschreiten.

25. **§ 43** erlaubt den **Datenabgleich.** Absatz 1 Satz 1 entspricht dabei nicht mehr einem modernen Verständnis der hinreichenden Bestimmtheit einer Datenverarbeitungsnorm. Es fehlt schlichtweg an tatbestandlichen Anforderungen an die Norm, nicht zuletzt, weil die Zweckbestimmung der Abgleichsdatei für die Betroffenen in keiner Weise erkennbar ist. Auch Satz 2 leidet daher unter einem **Bestimmtheitsmangel**.

26. Mit Blick auf die Regelungen zum **Kfz-Kennzeichenabgleich** in **§ 43a** ist nicht erkennbar, wie der GE (S. 212) zur der Einschätzung gelangt, schon die bisherige Regelung habe den Anforderungen des BVerfG in seiner neuen Entscheidung zur Kennzeichenerkennung genügt. Inhaltlich begründet wird dies nicht und ist nach der hier vertretenen Auffassung nicht zutreffend.

§ 43a I Nr. 3 und 4 erlauben – vergleichbar zur rechtswidrigen Praxis in Brandenburg mit derzeit rund 40 Millionen gespeicherten Kfz-Daten – einen **Massenabgleich** von Kfz-Kennzeichen gegen Jede*n die oder der zufällig die betroffene Straße nutzt, wenn nur **eine Person** zur polizeilichen Beobachtung oder Kontrolle **ausgeschrieben** ist. Dies verletzt das **Übermaßverbot**, zumal die Maßnahme nicht zur Abwehr von (konkreten) Gefahren dient. Nichts anderes gilt für **§ 45 V**.

§ 43 I Nr. 5 lässt **Lageerkenntnisse** der Polizei für eine Massenüberwachung ausreichen. Lageerkenntnisse sind Schlussfolgerungen und Einschätzungen der Polizei; ob und welchem Umfange diese eine **Tatsachenbasis** voraussetzen, lässt sich dem Gesetz nicht entnehmen. **§ 43 I Nr. 6** enthält keine **zeitlichen Begrenzungen** und erlaubt damit eine Dauerüberwachung eines erheblichen Teils des Territoriums des Landes, der teilweise eine Entfernung von über 40 km von der Bundesgrenze (Küste) erfasst.

27. § **45a III** gestattet selbst über den Zeitraum von **10 Jahren** (seit dem letzten Eintrag) hinaus eine weitere Speicherung personenbezogener Daten soweit und solange eine „**weitere Aufbewahrung**“ **erforderlich** sei. Tatbestandliche Voraussetzungen spezifischer Art fehlen hier. Dies steht durchaus im Einklang mit den Regelungen in anderen Bundesländern, ist aber aus Sicht des (**zeitlichen**) **Übermaßverbots** problematisch, da auch die in Absatz 2 genannten **Prüffristen nicht absolut** sind, sondern „regelmäßig mit dem Tag der letzten behördlichen Speicherung“ neu zu laufen beginnen. Dies erlaubt im Ergebnis ggf. unterschiedslos aus Gründen der Gefahrenabwehr, der Verhütung von Straftaten, der Verhütung von Ordnungswidrigkeiten etc. eine Speicherung personenbezogener Daten über Jahrzehnte hinweg; noch dazu ohne kürze Fristen zumindest für **besondere Kategorien personenbezogener Daten**. Zudem werden **keinerlei materielle Kriterien für die Dauer der Speicherung** festgelegt, mit Ausnahme der Differenzierung nach Lebensalter.

28. Die Maßgabe eines **hohen Risikos** für die Rechtsgüter der betroffenen Person in der Regelung zur **Datenschutz-Folgeabschätzung** in **§ 45b** entspricht zwar der JI-RL, stellt aber aus meiner Sicht eine zu hohe tatbestandliche Anforderung dar, nicht zuletzt mit Blick auf die im deutschen Recht eher ungewöhnliche Begrifflichkeit.

    Im Sinne einer **Vorsorge** gegen Verletzungen des Rechts auf informationelle Selbstbestimmung wie auch das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer System sollte hier eine **deutlich niedrige Schwelle** für eine verpflichtende Datenschutz-Folgenabschätzung gesetzlich verankert werden. Zudem sollte zwingend die/der **Landesbeauftragte für Datenschutz** beteiligt werden, um frühzeitig auch ein externes Feedback zu erhalten und mögliche Beanstandungen der Durchführung in einem späteren Zeitraum proaktiv zu vermeiden. Zudem sollte eine Veröffentlichung der Ergebnisse der Datenschutz-Folgeabschätzung gesetzlich zwingend vorgeschrieben werden (zu weiteren Anregungen für eine datenschutzfreundliche Umsetzung der JI-RL siehe am Ende).

29. Die **Benachrichtigungspflichten** in § 46a I erfassen keine nicht erkennbaren oder nicht offenen Eingriffe in das **Grundrecht auf informationelle Selbstbestimmung**, was auch zu einer Verkürzung des Rechts auf Rechtsschutz aus **Art. 19 IV GG** führen kann. So ist zum Beispiel in der Polizeipraxis gang und gäbe, dass Betroffene häufig nicht über die Durchführung eines **Datenabgleichs** in Kenntnis gesetzt werden und diesen daher allenfalls mit einem hohen Aufwand und auch Prozessrisiko der verwaltungsgerichtlichen Kontrolle zuführen können. Hier ist mit Blick auf die vorgenannten Grundrechte eine Ergänzung des GE notwendig.

    Die in **§ 46a II** 2 geregelte **Ausnahme von der Benachrichtigungspflicht** geht nach der Rechtsprechung deutlich zu weit, soweit allein eine weitere

Verwendung von Polizeibeamt*innen oder Vertrauenspersonen geschützt werden soll.

Zudem ist bei dem in Bezug genommenen **Absatz 2 Satz 1 Nr. 2**, der den Einsatz technischer Mittel betrifft, nicht erkennbar, woraus sich hier die Gefährdung ergeben soll; dies gilt auch für den Verweis auf § 33b IX, der allein einen weiteren Verweis enthält. Hier dürfte ein Fehler in der Verweisung selbst vorliegen.

In **§ 46a III Nr. 4** genügt nicht allein die Bezeichnung der **Kategorien der Empfänger,** insbesondere wenn diese im Ausland sich befinden, weil so ein möglicher Versuch des Rechtsschutzes gegen eine Speicherung beim Empfänger nicht oder nur unter erheblich erschwerten Voraussetzungen möglich ist. Es besteht hier ein Konflikt mit den materiellen Garantien aus Art. 19 IV GG. Vielmehr sind die Empfänger übermittelter Daten genau zu benennen.

30. **§ 46g** lässt eine Umsetzung der Anforderungen aus Art. 7 I JI-RL vermissen. Es ist für personenbezogenen Daten eine deutliche Unterscheidung zwischen **faktenbasierten Daten** und auf **persönlichen Einschätzungen** beruhenden Daten im Gesetz zu verankern.

31. Mit Blick auf die Anforderungen an die Gesetzmäßigkeit der Verwaltung und auch die Transparenz behördlichen Handelns erscheint die in **§ 46k** erlaubte **Auftragsdatenverarbeitung** zwar richtlinienkonform und auch nach deutschem Datenschutzrecht möglich, aber höchst problematisch, insbesondere soweit hier eine **Auslagerung der polizeilichen Datenverarbeitung auf Private** erlaubt werden soll.

32. **§ 48b** I regelt die **Befugnisse des Landesbeauftragten für Datenschutz** über die polizeiliche Datenverarbeitung und **beschränkt** diese massiv gegenüber den Regelungen in Art. 58 DSGVO. Dies ist mit dem Erwägungsgrund 82 der JI-RL schwerlich vereinbar: „Um die wirksame, zuverlässige und einheitliche

Überwachung der Einhaltung und Durchsetzung dieser Richtlinie in der gesamten Union gemäß dem AEUV in der Auslegung durch den Gerichtshof sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben, darunter Untersuchungsbefugnisse, Abhilfebefugnisse und beratende Befugnisse, die notwendige Instrumente zur Erfüllung ihrer Aufgaben darstellen."

Gerade die geforderten **Abhilfebefugnisse** hat der Gesetzgeber aber mit Blick auf die Befugnisse nach Absatz 2 und 3 der DSGVO erheblich eingeschränkt. Ob dies europarechtlich zulässig ist, kann hier nicht geprüft werden; dem Sinn und Zweck der JI-RL läuft eine solche Beschränkung – auch unter Beachtung der Regelungen in § 48b III – zuwider.

33. Das in **§ 48h** vorgesehene „**SOG-Gremium**" erscheint hinsichtlich seiner Mitgliederzahl, noch dazu bei einer Verteilung der Sitze nach Stärkeverhältnis der Fraktionen, mit Blick auf die steigende Zahl von im Parlament vertretenen Parteien **zu klein bemessen**.

34. Die in **§ 67b** gestattete **Aufenthaltsanordnung** soll einerseits zur Abwehr konkreter Gefahren, andererseits aber auch zur Verhütung so genannter terroristischer Straftaten zulässig sein. Die Maßnahme stellt nach der hier vertretenen Auffassung einen erheblichen **Eingriff** in die **Freiheit der Person** und **nicht nur die Freizügigkeit** dar, weil die Untersagung, sich aus einem bestimmten Bereich zu entfernen, dessen minimale Begrenzung im Gesetz nicht weiter bestimmt ist, dazu führen könnte, dass sogar ein Wohngrundstück, ein Straßenblock oder ein isoliert auf dem Lande stehendes Wohngebäude nicht mehr verlassen werden darf. Dies kommt einer Freiheitsentziehung gleich oder sehr nahe und überschreitet daher nach der hier vertretenen Auffassung den sachlichen Anwendungsbereich des Art. 11 GG.

Aber auch bei Anwendbarkeit dieser Norm fragt sich, ob die monatelange „Verbannung" an einen bestimmten Ort an sich verhältnismäßig sein kann und

ob diese für 3 Monate allein durch die **Polizei ohne richterliche Vorabkontrolle** angeordnet werden kann.

Auch ansonsten enthält die Regelung nicht hinreichend bestimmte Beschränkungen, wenn etwa in Absatz 3 Nr. 2 geregelt wird, die Person dürfe den Geltungsbereich der Anordnung nicht ohne „**Erlaubnis**“ der Polizei verlassen, ohne dass das Gesetz auch nur im Ansatz festlegen würde, ob es sich hierbei um einen eigenständigen Verwaltungsakt handeln soll und vor allem, unter welchen Voraussetzungen hierauf aus Sicht des Betroffenen ein Anspruch besteht. Diese ist ein klarer **Verstoß gegen das Gebot der Normenklarheit**.

35. Zum Schluss erlaube ich mir neben den oben aufgezeigten Schwächen oder auch Abweichungen von der JI-RL noch einige Anmerkungen zur **Umsetzung des EU-Datenschutzrechts** im Entwurf. Dieser ist aus meiner Sicht auf eine eher an Minimalanforderungen orientierten Umsetzung ausgerichtet, statt die vom EU-Recht ohnehin geforderte Stärkung und Neuordnung des Datenschutzes proaktiv anzugehen:
    a. Es fehlt eine Pflicht zu periodisch zu wiederholenden **Technikfolgenabschätzungen** der zulässigen Maßnahmen der Datenerhebung und der Datenverarbeitung.
    b. Die Anforderungen an **Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen** werden nur abstrakt im Gesetz wiederholt, statt diese in konkreten gesetzliche Maßgaben und ggfs. weiteren technisch-organisatorische Normen im Verordnungswege detaillierter vorzugeben.
    c. Die Befugnisse des **Landesdatenschutzbeauftragten** sollten deutlich gestärkt werden, bis hin zu Anordnungsbefugnissen.
    d. **Automatisierte Entscheidungen** durch die Polizei sollten gesetzlich ausgeschlossen werden.
    e. Der rechtliche Grundsatz der Zweckbindung in der Datenerhebung und -verarbeitung sollte gestärkt werden.

f. **Neue polizeiliche Befugnisse** sollten generell **zeitlich befristet** werden mit der Pflicht zu einer anschließenden externen wissenschaftlichen Evaluation bei Bestellung des/der Sachverständigen durch den Landtag. Erst danach kann eine Entfristung erfolgen.

g. Es sollte regelmäßig **evaluiert** werden, welche der **bestehenden Befugnisse** (zur Datenverarbeitung) überhaupt in welchem Umfang und mit welchem Erfolg von der Polizei genutzt werden (zur Durchführung siehe vorstehend).

h. Die Verarbeitung **besonderer Kategorien personenbezogener Daten** sollte durch den Gesetzgeber dahingehend spezifizieren werden, dass dieser einen Katalog der so verarbeitenden Daten im Gesetz verankert oder es ist die Pflicht zum Erlass einer entsprechenden Rechtsverordnung im Gesetz zu verankern.

i. Die Prüffristen sind in **Höchstspeicherfristen** umzuwandeln und deutlich zu verkürzen. Soll bei im Gesetz ausdrücklich mit spezifizierten Tatbestandsvoraussetzungen vorgesehenen Ausnahmen länger gespeichert werden, wäre eine Pflicht zur Unterrichtung und Begründung dem Betroffenen gegenüber im Gesetz zu verankern.

j. Die **Verzeichnisse zur Datenverarbeitung** sind öffentlich zu machen.

k. Die Zweckänderung von **Protokolldaten** für andere Zwecke als die der Strafverfolgung, ist in Übereinstimmung mit Art. 25 JI-RL zu unterbinden.

Aus zeitlichen Gründen war eine weitergehende Befassung mit dem GE hier leider nicht möglich. Soweit Normen nicht Gegenstand der Betrachtung waren, kann dies daher nicht so verstanden werden, dass allein die hier kommentierten Normen aus Sicht des Unterzeichners Rechtsprobleme aufweisen.