Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin

Vor dem Hintergrund der kurzfristigen Einladung zur Anhörung am 29. September 2025 nimmt die BlnBDI nur zu ausgewählten Normen des o.g. Gesetzes im Folgenden Stellung:

§ 24a: Datenerhebung an und in gefährdeten Objekten

Mit der Vorschrift werden auch Amts- und Dienstgebäude als gefährdete Objekte benannt und die Möglichkeit der Videoüberwachung auf Innenräume von gefährdeten Objekten ausgeweitet.

Im Hinblick auf die im Normtext aufgenommenen Amts- und Dienstgebäude verweist die Begründung darauf, dass es sich dabei auch um gefährdete Gebäude handeln *kann*. Als Beispiele werden Gebäude von Bundes- oder Landesverwaltung einschließlich solcher der Sicherheitsbehörden genannt, „sofern die entsprechende Gefährdungsbewertung vorliegt“ (S. 158 der Begründung des Entwurfs). Im Weiteren heißt es dann, dass es für die Gefährdungsbewertung um eine Gefährdung von Objekten „dieser Art“ geht, so wie auch im Normtext formuliert. Voraussetzungen für die Maßnahme sei somit weder, dass Straftaten gerade an dem zu überwachenden Objekt erwartet werden, noch dass konkrete Hinweise auf bevorstehende Straftaten oder tatsächliche Anhaltspunkte bestehen, dass bestimmte Straftaten drohen. Die Formulierung zu den Amts- und Dienstgebäuden im Normtext legt nahe, dass Amts- und Dienstgebäude immer gefährdete Objekte im Sinne der Norm darstellen („insbesondere“). Insofern stellt sich für die Amts- und Dienstgebäude die Frage, ob es auf der Basis des Normtextes überhaupt Situationen geben kann, in denen eine Videoüberwachung **nicht** gerechtfertigt wäre: Die Gefährdungsbewertung basiert im Wesentlichen auf der „Art“ des Objekts und das Objekt ist im Normtext selbst als Regelbeispiel für ein gefährdetes Objekt aufgeführt. Auf die tatsächlichen Gegebenheiten vor Ort kommt es nicht an.

Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI)
Alt-Moabit 59-61, 10555 Berlin
Eingang: Alt-Moabit 60

Telefon: 030 13889-0
Telefax: 030 215 50 50
Sprechzeiten: Mo., Di., Fr. 10–12 Uhr,
Mi., Do. 13–15 Uhr und nach Vereinbarung

E-Mail: mailbox@datenschutz-berlin.de
Website: www.datenschutz-berlin.de

Diese erweiterte Möglichkeit der Videoüberwachung in und an Amts- und Dienstgebäuden stellt eine Änderung zur bisherigen Rechtslage dar, die nicht nur „klarstellender“ Natur ist (S. 158 der Begründung zum Entwurf, „wird klarstellend ergänzt“). Insofern lässt die Begründung nicht erkennen, auf welcher (Evidenz-)Basis Amts- und Dienstgebäude generell als gefährdete Objekte einzustufen sind.

Zudem bleibt unklar, wie eine solche regelhafte Möglichkeit der gefahrenabwehrrechtlichen Videoüberwachung an Amts- und Dienstgebäuden mit der Regelung nach § 20 BlnDSG vereinbar ist. Dieser regelt die Videoüberwachung öffentlicher Räume bereits für Zwecke des Hausrechts oder zur Erfüllung öffentlicher Aufgaben mit einer Interessenabwägung und strikteren Löschfristen. Die Videoüberwachung von Amtsgebäuden zeigt sich hier als Eigensicherungsmaßnahme und damit als Verwaltungsaufgabe und nicht als polizeiliche Gefahrenabwehr. Die polizeirechtliche Ermächtigung des § 24a sollte nicht dazu dienen können, diese datenschutzrechtlichen Beschränkungen zu umgehen. Insgesamt empfehlen wir daher die Erweiterung auf Amts- und Dienstgebäude in ihrer regelhaften Formulierung zu streichen.

Die Erweiterung der Videoüberwachung auf Innenräume rechtfertigt die Begründung mit einer „möglichst zielgenaue[n] und damit grundrechtsschonende[n]“ Videoüberwachung (S. 157 f. der Begründung des Entwurfes). Unberücksichtigt bleibt dabei – jedenfalls soweit der Begründung zu entnehmen – die Abwägung mit der besonderen Grundrechtsausübung innerhalb von Räumlichkeiten etwa bei der Videoüberwachung in Innenräumen von Religionsstätten. Insofern kann die Videoüberwachung eine abschreckende Wirkung entfalten, die in der Grundrechtsabwägung jedenfalls Berücksichtigung finden muss. Gerade in solchen Fällen könnte die Maßnahme durch eine konkrete Gefährdungsbewertung und nicht nur nach „Art“ des Gebäudes eingehegt werden. Die Ausweitung auf Innenräume sollte daher unter strengeren Voraussetzungen und mit expliziten Schutzvorkehrungen für die Grundrechtsausübung erfolgen.

Die Verlängerung der Speicherdauer von „unverzüglicher Löschung“ auf einen Monat stellt eine erhebliche Intensivierung des Grundrechtseingriffs dar, ohne dass dies näher begründet wird. Die Videoüberwachung im öffentlichen Raum betrifft fast ausschließlich Personen, die zu der Maßnahme keinen Anlass geboten haben. Die geplante Änderung übersteigt die bisher übliche Höchstspeicherdauer von 48 Stunden ohne erkennbaren Grund erheblich.

Unklar ist die Regelung in Absatz 3, wonach Daten nicht gelöscht werden müssen, wenn Tatsachen die Annahme rechtfertigen, dass „die Person“ künftig Straftaten von erheblicher Bedeutung begehen wird. Hier erschließt sich nicht, wer „die Person“ ist und wie diese im Zusammenhang mit der Überwachung eines gefährdeten Objekts Anlass zu einer „prognostischen Gefährlichkeit“ gegeben hat. Die Aufnahmen zum Schutz von gefährdeten Objekten werden mit dieser Vorgabe zur verlängerten Speicherung zu einer auf eine Person ausgerichtete Überwachungsmaßnahme, wobei die im Raum stehenden zukünftigen erheblichen Straftaten nicht auf solche begrenzt bzw. bezogen sind, die am gefährdeten Objekt begangen werden.

Die Vorschrift wurde offensichtlich aus § 24 Abs. 2 übernommen. Dort hat sie einen Anknüpfungspunkt, da sie sich auf Teilnehmende einer Versammlung bezieht. Im Kontext des § 24a fehlt es allerdings an einem solchen. Insofern erschließt sich nicht, welches Szenario hier zugrundegelegt wurde und inwieweit hiermit überhaupt noch eine präventive Tätigkeit im Gefahrenabwehrrecht vorliegt. Vor diesem Hintergrund ist für uns nicht abschließend prüfbar, ob die formulierte Eingriffsschwelle als einhegendes Kriterium ausreichend sein kann oder ob es nicht weitergehender kompensatorischer Maßnahmen für diese auf eine Person ausgerichtete Maßnahme bedarf (etwa einer richterlichen Zustimmung). Insofern zählt die Benachrichtigungspflicht nach § 24a Abs. 4 kaum als kompensatorische Maßnahme, da diese nach den Vorgaben des Abs. 4 regelmäßig ausgeschlossen sein dürfte. Zu einer Verhütung von Straftaten ist eine Verlängerung der Speicherdauer letztlich nicht erforderlich. Soweit mit der Vorschrift verdächtiges Vortatverhalten (etwa Ausspähen der Örtlichkeit) gemeint ist, kann polizeirechtlich umgehend reagiert werden.

Insgesamt ist bei allen Maßnahmen, die aus den verschiedenen Videoüberwachungsbefugnissen heraus übergreifend eine Verlängerung der Speicherdauer auf der Grundlage einer prognostischen Gefährlichkeit ermöglichen zu beachten, dass diese Maßnahmen ein über die Einzelmaßnahme hinausgehendes Eingriffsgewicht als Gesamtheit entfalten, da sie unabhängig vom eigentlichen Anknüpfungspunkt fortbestehen. Diese Gesamtbetrachtung bleibt weitestgehend unberücksichtigt im Entwurf.

Schließlich sollte der Verweis auf die automatisierte Auswertung von Verhaltensmustern entfallen, da diese Form der biometrischen Datenverarbeitung unverhältnismäßig in das Recht auf informationelle Selbstbestimmung eingreift (dazu bei § 24e Abs. 4).

§ 24c: Bild- und Tonaufnahmen und -aufzeichnungen zur Eigensicherung und zum Schutz von Dritten

In § 24c Absatz 8 Satz 2 wird der gerichtliche Prüfungsgegenstand von Bild-und Tonaufnahmen der Bodycams an nicht öffentlich zugänglichen Orten auf die Datenerhebung beschränkt. Bisher musste das Gericht die Rechtmäßigkeit der beabsichtigten Nutzung prüfen und damit inzident auch die Rechtmäßigkeit der Datenerhebung. Künftig soll das Gericht nur noch die Rechtmäßigkeit der bereits erfolgten Datenerhebung prüfen, nicht mehr die Rechtmäßigkeit der beabsichtigten Datennutzung. Die Begründung verweist auf Art. 13 Abs. 5 Satz 2 GG als Vorbild (vgl. S. 164 der Begründung des Entwurfes). Zu berücksichtigen ist hierbei zweierlei: Zum einen gehen die Zweckbestimmungen des § 24c Abs. 7 Satz 4 bereits über jene Zwecke hinaus, die in Art. 13 Abs. 5 Satz 2 GG genannt sind(Gefahrenabwehr und Strafverfolgung). Weiterhin soll die Zweckbindung in § 24c Absatz 8 Satz 1 i.V.m. § 24c Abs. 7 Satz 4 nicht ausschließen – so die Begründung zum Entwurf (S. 162) – dass u.a. die §§ 42c und 42d unberührt bleiben. Dies ermöglicht es, Bodycam-Aufzeichnungen über die zulässige Speicherdauer hinaus zu Aus- und Fortbildungszwecken, für Forschungszwecke, für archivarische Zwecke sowie zum Trainieren und Testen von KI-Systemen zu nutzen. Insofern sollte es in jedem Fall dabei bleiben, dass die bisherige umfassenden richterliche Kontrolle sowohl der Datenerhebung als auch der Datennutzung beibehalten wird.

§ 24e: Datenerhebung an kriminalitätsbelasteten Orten

Der neue § 24e ermöglicht der Polizei die Videoüberwachung an kriminalitätsbelasteten Orten zur vorbeugenden Kriminalitätsbekämpfung. Sie stellt damit als Vorsorgemaßnahme kein Mittel der konkreten Gefahrenabwehr oder der Verhütung bestimmter Straftaten dar. Die Maßnahme erfolgt auf Anordnung der Polizeipräsidentin oder des Polizeipräsidenten und unterliegt einer mindestens alle zwei Jahre zu erfolgenden Überprüfung ihrer Auswirkungen auf die Kriminalität am jeweiligen Ort. Nach § 17a Abs. 1 werden kriminalitätsbelastete Orte grundsätzlich durch Rechtsverordnung der für Inneres zuständigen Senatsverwaltung festgelegt. In Eilfällen kann die Polizeipräsidentin oder der Polizeipräsident für maximal einen Monat im Kalenderjahr eine entsprechende Allgemeinverfügung erlassen.

Die materiellen Voraussetzungen für die Einstufung als kriminalitätsbelasteter Ort bleiben niedrigschwellig. Es müssen lediglich Tatsachen die Annahme rechtfertigen, dass dort Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben. Die Definition erheblicher Straftaten aus § 17 Abs. 3 ist weit gefasst. Insbesondere die dortige Verweisung auf den Katalog nach § 100a Abs. 2 StPO umfasst etwa die Fälschung von Zahlungskarten und Schecks (§ 152a StGB), die Bestechlichkeit und Bestechung von Mandatsträgern (§ 108e StGB), wettbewerbsbeschränkende Absprachen bei Ausschreibungen (§ 298 StGB), den Bankrott (§ 283a StGB) und verschiedene Formen der Urkundenfälschung (§ 267 StGB), alles Vorwürfe, die weder in einem erkennbaren Zusammenhang mit einer Videoüberwachung stehen, noch zu eingriffsintensiven, breit gestreuten Maßnahmen der Gefahrenabwehr drängen. Diese Kataloge sollten unter gefahrenabwehrrechtlichen Gesichtspunkten angepasst werden. Insofern würde die Eingriffshürde von einem spezifischen Katalog profitieren, der sich erkennbar am Schutz klar abgrenzbarer Rechtsgüter orientiert.

Darüber hinaus stellt die Frage, welche Orte in Berlin als kriminalitätsbelastete Orte definiert werden, eine für die Eingriffsschwelle sehr wesentliche Konkretisierung dar. Insofern ist es nach unserer Ansicht erforderlich, dass diese wesentliche Entscheidung durch das Parlament getroffen wird und nicht „nur“ Gegenstand einer Verwaltungsverordnung ist. Die Videoüberwachung öffentlicher Räume führt zu unterschiedslosen Eingriffen in das Grundrecht nahezu aller Personen, die sich an diesen Orten aufhalten, ohne dass diese für die Überwachungsmaßnahme einen Anlass gesetzt haben. Es ist zu befürchten, dass diese Regelung zu einer Videoüberwachung hochfrequentierter Bereiche insbesondere der Innenstadt Berlins führt. Zur Pflicht der öffentlichen Bekanntmachung der Orte der Videoüberwachung heißt es in der Begründung (S 166):

„Sie ermöglicht es nämlich schon vorab feststellen zu können, an welchen Orten Bildaufnahmen oder - aufzeichnungen gefertigt werden. Wer solche Aufnahmen vermeiden will, kann den betroffenen Orten ausweichen…“

Es wurde damit durchaus erkannt, dass Personen das Bedürfnis haben könnten, der Videoüberwachung auszuweichen. In den engen räumlichen Verhältnissen von Berlin kann dies aber dazu führen, dass bei mehreren angrenzenden kriminalitätsbelasteten Orten größere Bereiche des öffentlichen Raums für solche Personen nicht mehr nutzbar wären

und Rückzugsräume weniger würden. Sofern etwa, z.B. in Parks, von einem kriminalitätsbelasteten Ort ausgegangen wird, müssten Personen auf die Freizeitnutzung in dem Park verzichten, wenn sie der Videoüberwachung ausweichen wollen. Hier spielen Erwägungen der Eingriffe in die Grundrechte vieler unbeteiligter Dritter für die Verhältnismäßigkeit der Maßnahme eine Rolle. Vor der Installation einer Videoüberwachungsanlage sind zumutbare Alternativen zu prüfen. Bauliche Maßnahmen, Ausleuchtung, regelmäßige Kontrollgänge von Sicherheitspersonal, Notfall- oder Alarmknöpfe können ggf. vor bestimmten Straftaten schützen. In Frage steht, ob durch die offene Überwachungsmaßnahme Straftaten tatsächlich verhindert oder nur verlagert werden. In der Norm des § 24e findet sich jedenfalls kein tatbestandlicher Anknüpfungspunkt für die Prüfungen der Verhältnismäßigkeit. Den einzigen tatbestandlichen Anknüpfungspunkt stellt insofern der Begriff des kriminalitätsbelasteten Ortes und die in § 17a Abs. 1 Satz 2 vorgesehene Eingriffsschwelle dar, was umso mehr dafür spricht, dass die Einstufung eine dem Parlament vorbehaltene wesentliche Entscheidung darstellt.

§ 24e Absatz 3 verweist auf die entsprechende Anwendung von § 24a Absatz 3 und 4. Hierzu wird auf die Ausführungen zu § 24a entsprechend verwiesen.

24e Abs. 4: Automatisierte Verhaltensmustererkennung

§ 24e Abs. 4 führt erstmals eine Rechtsgrundlage für die automatisierte Auswertung von Bildaufnahmen zur Erkennung von Verhaltensmustern ein, die auf Straftaten oder Unglücksfälle hindeuten können. Die Regelung ist methodenoffen ausgestaltet und schließt den Einsatz künstlicher Intelligenz nicht aus. Nach der Begründung soll die automatisierte Mustererkennung lediglich dazu gedacht sein, jene Polizeivollzugsbeamtinnen und -beamten, die ein Einsatzgeschehen über Bildschirme betrachten, bei ihrer Aufmerksamkeit mit einem Assistenzsystem zu unterstützen (vgl. S. 168 der Begründung des Entwurfes). Trotz der dortigen Bezeichnung als Assistenzsystem ist offenbar keineswegs nur eine aufmerksamkeitsunterstützende Live-Auswertung gemeint. Vielmehr nennt der Gesetzentwurf die Auswertung der (gespeicherten) Bildaufzeichnungen ausdrücklich neben der Auswertung der (übertragenen) Bildaufnahmen. Die Vorschrift ermöglicht so die retrograde Auswertung gespeicherter Bildaufzeichnungen über einen Zeitraum von bis zu einem Monat, in Einzelfällen länger. Dies eröffnet, insbesondere im Zusammenhang mit dem Einsatz verfahrensübergreifender Analyseplattformen in § 47a, qualitativ völlig neue Möglichkeiten der systematischen Analyse von Bewegungsmustern, Sozialkontakten und Verhaltensweisen von Passanten.

Auch handelt es sich bei den Videoaufnahmen und den Informationen von Verhaltensmustern um Daten, die nach § 42d für das KI-Training grundsätzlich weiterverwendet werden dürfen. Hier bleibt nach unserer Auffassung offen, für welche Einsatzszenarien diese im Zusammenhang mit kriminalitätsbelasteten Orten erhobenen Informationen in das Training eines KI-Systems einfließen dürfen und wann die Daten nach § 24e Abs. 3 dann tatsächlich gelöscht werden, denn auch hier gilt: Personenbezogene Daten, die zum Training eines KI-Modells verwendet wurden, lassen sich schwerlich aus dem Modell entfernen.

Wenn die Regelung des § 24e Abs. 3 aber – wie in der Begründung nahegelegt - nur die beschriebenen Assistenzsysteme im Blick hat, muss dies in der Norm selbst als Zweckbindung der Auswertungsmöglichkeiten (etwa Optimierung der Verhaltensmustererkennung) insbesondere für die retrograde Auswertung gespeicherter Bildaufzeichnungen zum Ausdruck kommen. Diese Zweckbindung müsste dann entsprechend auch für die personenbezogene Datenverarbeitung nach § 42d bzw. § 47 gelten. Andernfalls muss ganz konkret beschrieben und geregelt werden, unter welchen Bedingungen die Befugnisse nach § 24e etc. eigentlich auch dazu dienen, Trainingsdaten für KI-Systeme zu generieren.

Der Gesetzentwurf erweitert die automatisierte Verhaltensmustererkennung über § 24e hinaus durch Verweisungen in anderen Normen. § 24a Abs. 1 Satz 2 ermöglicht die Anwendung bei der Videoüberwachung gefährdeter Objekte, während § 24f Satz 4 den Einsatz bei Übersichtsaufnahmen zur Einsatzvorbereitung, -lenkung und -leitung vorsieht und § 24 Abs. 1 Satz 4 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen einbezieht. Diese systematische Ausweitung verstärkt die datenschutzrechtlichen Bedenken, da die Verhaltensmustererkennung damit in nahezu allen Bereichen der polizeilichen Videoüberwachung zum Einsatz kommt. Die Auswertung wird insbesondere in der Generalklausel zum Einsatz von Drohnen in § 24g nicht ausgeschlossen. Diese umfassende Vernetzung schafft ein flächendeckendes System automatisierter Verhaltensüberwachung und ist insbesondere nicht auf sog. „Angsträume“ beschränkt sondern wird durchgängig dazu führen, dass Unbeteiligte ihr Verhalten in der Öffentlichkeit anpassen und ggf. dennoch - aufgrund der zu erwartenden Fehleranfälligkeit - Ziel polizeilicher Maßnahmen werden. Eine solche Gesamtbetrachtung ist dem Entwurf nicht zu entnehmen.

§§ 25a, 25b: Verdeckter Einsatz technischer Mittel

Die neuen §§ 25a und 25b schaffen eigenständige Rechtsgrundlagen für den verdeckten Einsatz technischer Mittel außerhalb von Wohnungen (§ 25a) und in oder aus Wohnungen (§ 25b).

Beide Vorschriften verweisen durch ihre Anknüpfung an § 25 Absatz 1 auf die Straftatenkataloge nach § 100a Absatz 2 StPO (für § 25a Absatz 2) und § 100b Absatz 2 StPO. Auch hier ist zu prüfen, ob diese Kataloge unter gefahrenabwehrrechtlichen Gesichtspunkten angepasst werden können. Insofern würde die Eingriffshürde von einem spezifischen Katalog profitieren, der sich erkennbar am Schutz klar abgrenzbarer Rechtsgüter orientiert.

§ 26a: Datenerhebung durch Telekommunikationsüberwachung informationstechnischer Systeme

Der neue § 26a schafft für Berlin erstmals eine präventiv-polizeiliche Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) in Berlin. Die Befugnis ermöglicht der Polizei, durch technische Eingriffe in informationstechnische Systeme verschlüsselte Telekommunikation vor der Verschlüsselung zu überwachen und aufzuzeichnen.

Ein zentraler datenschutzrechtlicher Kritikpunkt betrifft die unzureichende Regelung der Verwendung unbekannter Schwachstellen. § 26a Absatz 2 enthält zwar wichtige technische Sicherungsvorgaben, regelt jedoch die Erstausnutzung bisher noch nicht geschlossener Programmschwachstellen (sog. Zero-Day-Exploits) nicht ausdrücklich. Das Bundesverfassungsgericht hat in seiner Rechtsprechung zum Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme die besondere Schutzbedürftigkeit dieser Systeme hervorgehoben und die staatliche Schutzpflicht für die IT-Sicherheit betont. Es kann daher nicht davon ausgegangen werden, dass die Verwendung von Zero-Day-Exploits vor dem Hintergrund der staatlichen Schutzpflicht ohne Weiteres zulässig ist, wenn sie in der Ermächtigungsgrundlage nicht hinreichend bestimmt und benannt ist. Es ist dem Staat zwar erlaubt, für den Erfolg verdeckter Maßnahmen alle verhältnismäßigen und erlaubten Mittel einzusetzen. Es ist dem Staat allerdings nicht erlaubt, bekannte Sicherheitslücken für den Erfolg verdeckter Maßnahmen bewusst bestehen zu lassen, wenn davon der Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aller

anderen, unbescholtenen Bürger:innen betroffen ist. Die Ausnutzung einer Schwachstelle durch den Staat ist nur dann verhältnismäßig, wenn der Staat gleichzeitig den Hersteller über die Schwachstelle informiert, so dass diese geschlossen werden kann. Insofern sollte § 26a Absatz 2 Satz 1 um eine Nummer 4 ergänzt werden, die klarstellt, dass Schwachstellen in Programmsystemen, die deren Herstellern noch nicht bekannt sind, nur ausgenutzt werden dürfen, wenn entsprechende Schwachstellen unverzüglich den Herstellern gemeldet werden.

Schließlich sollte bei der Nutzung fremder Endgeräte nach § 26a Absatz 1 Nummer 3 explizit geregelt werden, dass nur Kommunikation der betroffenen Person erfasst werden darf.

Für die Datenerhebung durch verdeckten Eingriff in informationstechnische Systeme in § 26b, die unter den gleichen Voraussetzungen wie in § 26a Absatz 1 zulässig sein soll, gelten diese Ausführungen entsprechend.

§ 26e: Funkzellenabfrage

Die vorgeschlagene Regelung führt eine neue Befugnisnorm zur Funkzellenabfrage ein, die der Polizei ohne Wissen der Betroffenen die Erhebung aller in einem bestimmten Zeitraum in einem bestimmten örtlichen Bereich in Funkzellen angefallenen Telekommunikationsverkehrsdaten ermöglicht. Diese umfassen insbesondere Daten darüber, wer, wann, wo mit wem kommuniziert oder zu kommunizieren versucht hat, einschließlich Rufnummern, Kommunikationsdiensten, Beginn und Ende von Verbindungen, Datum und Uhrzeit sowie übermittelten Datenmengen.

Die Befugnis soll unter drei alternativen Eingriffsvoraussetzungen zulässig sein: Erstens zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben, Freiheit oder sexuelle Selbstbestimmung einer Person sowie für Sachen von bedeutendem Wert. Bei den Straftaten gegen die sexuelle Selbstbestimmung ist eine Mindeststrafandrohung von sechs Monaten vorgesehen. Zweitens zur Verhütung von Straftaten aus dem Katalog des § 100g Absatz 2 StPO, wenn Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf konkretisierte Weise eine besonders schwerwiegende Katalogstraftat begehen wird. Drittens bei terroristischen Straftaten, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit terroristischer Straftaten begründet.

Die Funkzellenabfrage stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und das Telekommunikationsgeheimnis (Art. 10 GG) dar. Daneben können weitere Grundrechte wie die Berufsausübungsfreiheit von Berufsgeheimnisträger:innen aus Art. 12 GG, die Religionsfreiheit von Geistlichen aus Art. 4 GG, die Pressefreiheit von Journalisten aus Art. 5 Abs. 1 S. 2 GG oder das freie Mandat von Abgeordneten aus Art. 38 Abs. 1 S. 2 GG betroffen sein. In Großstädten wie Berlin würden regelmäßig die Kommunikationsdaten einer Vielzahl von unbeteiligten Personen erfasst. Auch die Begründung des Entwurfes erkennt diese erhebliche Streubreite an und beschreibt sie als charakteristisches Merkmal der Funkzellenabfrage in dicht besiedelten Gebieten (vgl. S. 216 der Begründung des Entwurfes). Es stellt sich hier insbesondere die Frage, ob eine solche weitreichende Maßnahme, die in die Grundrechte vieler unbeteiligter Personen eingreift, verhältnismäßig sein kann. Hierzu sieht Abs. 1 Satz 2 eine Subsidiaritätsklausel vor. Diese ist aus unserer Sicht unzureichend. Es fehlt etwa die Anforderung, dass festgestellt sein muss, dass andere polizeiliche Maßnahmen ausgeschöpft sind, bevor eine Funkzellenabfrage durchgeführt werden darf.

§ 26e Abs. 3 verweist für die Dauer der Maßnahme auf § 26b Abs. 7, wonach die Maßnahme auf höchstens einen Monat zu befristen ist mit der Möglichkeit dies um jeweils einen Monat zu verlängern. Diese lange Dauer erscheint insbesondere vor dem Hintergrund, dass es jedenfalls bei § 26e Abs. 1 Nr. 2 und 3 darum geht den Aufenthalt einer Person unmittelbar vor der vermuteten Tat festzustellen (vgl. S. 217 der Begründung des Entwurfes) sehr lang. Insofern lässt die Begründung nicht erkennen, auf welcher (Evidenz-)Basis davon ausgegangen wird, dass die Befristung der Maßnahme bis zu einem Monat erforderlich ist.

Auch für die Funkzellendaten gilt, dass diese sowohl nach § 47a auf einer Analyseplattform zusammengeführt bzw. für das KI-Training nach § 42d weiterverwendet werden könnten. Auch hier stellt sich wiederum die Frage, nach welchen Eingriffsschwellen erfolgt eine Weiterverwendung zum KI-Training bzw. wann werden diese Daten tatsächlich gelöscht. Durch die Verknüpfung der erhobenen Daten mit automatisierten Analyseplattformen lassen sich detaillierte Bewegungsprofile erstellen. Dies ermöglicht Rückschlüsse auf politische Aktivitäten, soziale Beziehungen und persönliche Gewohnheiten der Betroffenen.

Vor dem Hintergrund der sehr großen Streubreite der Maßnahme und der Eingriffe in die Grundrechte vieler unbeteiligter Personen, müssen die Eingriffsschwellen für diese Maßnahme erhöht werden und auf die Abwehr unmittelbar bevorstehender Gefahren für Leib, Leben, Freiheit und sexuelle Selbstbestimmung. Die Subsidiaritätsklausel muss dahingehend verschärft werden, dass ausdrücklich festgelegt wird, dass andere polizeiliche Maßnahmen ausgeschöpft sein müssen. Die Anordnungsdauer sollte auf höchstens 72 Stunden begrenzt werden. Darüber hinaus sollten spezielle Schutzvorschriften für Berufsgeheimnisträgerinnen und -träger vorgesehen werden. Die Schutzvorschriften in § 18a (Verwertungsverbot) sind insbesondere in Verbindung mit § 47a und § 42d unzureichend. Ich empfehle außerdem eine unverzügliche Benachrichtigungspflicht für alle von der Maßnahme erfassten Personen.

§ 28a: Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

Der neu eingefügte § 28a schafft eine Rechtsgrundlage für die biometrische Fernidentifizierung von Personen durch automatisierten KI-gestützten Abgleich von Gesichts- und Stimmdaten mit öffentlich zugänglichen Internetdaten. Die Regelung ermöglicht es der Polizei erstmals, im allgemein öffentlich zugänglichen Internet Personen anhand von Bildern oder Stimmen zu identifizieren.

Die Regierungsfraktionen begründen diese neue Befugnis mit dem Fall der mutmaßlichen Terroristin Daniela Klette, die trotz intensiver Fahndung über Jahre hinweg unentdeckt blieb, obwohl zahlreiche Fotos von Freizeitaktivitäten im Internet allgemein zugänglich waren (vgl. S. 237 der Begründung des Entwurfes). Investigativ tätige Journalisten hätten durch KI-gestützten Abgleich alter Fahndungsfotos mit öffentlich zugänglichen Internetfotos entscheidende Hinweise auf den aktuellen Aufenthaltsort geben können, während den Strafverfolgungsbehörden die erforderliche gesetzliche Befugnisnorm gefehlt habe (vgl. S. 237 der Begründung des Entwurfes).

Der vorgeschlagene Entwurf löst dieses Problem der Strafverfolgung nicht, sondern schafft stattdessen eine neue Befugnis im Gefahrenabwehrrecht.

Der neu vorgesehene § 28a stellt einen nicht unerheblichen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Die biometrische Fernidentifizierung durchbricht die Anonymität des Alltags und erfasst

Personen, deren Abbildungen im Internet zugänglich sind, in öffentlichen und in privaten Bereichen sowohl gezielt als auch ungezielt. Dies schafft ein Gefühl permanenter Überwachung und kann zu erheblichen Verhaltensanpassungen führen, das Bürger:innen weit über die Stadtgrenzen hinaus betrifft. Bei der biometrischen Datenverarbeitung handelt es sich um ein Verfahren mit besonders hohem Eingriffspotential, da biometrische Daten zur Messung und Analyse körperlicher Merkmale erhoben werden, die für jeden Menschen einzigartig sind.

Der Grundrechtseingriff betrifft dabei nicht nur die recherchierten Zielpersonen und Personen, die ihnen ähnlich sind, sondern eine unbestimmte Vielzahl unbeteiligter Personen. Dadurch wird gleichzeitig das Recht auf informationelle Selbstbestimmung derjenigen Personen berührt, deren öffentlich zugängliche Referenzdaten im Internet in den Abgleich einbezogen werden (vgl. Ogorek, LTZ 2024, 274, 278). Die Eingriffsintensität wird dadurch erheblich verstärkt, dass alle im Internet verfügbaren biometrischen Daten im Ergebnis als Referenzdatenbank fungieren, was praktisch großer Teile der Bevölkerung betrifft. Die Tragweite des Eingriffs wird durch den Einsatz künstlicher Intelligenz noch verstärkt. Der biometrische Abgleich soll mithilfe von KI automatisiert erfolgen, da nur durch technische Anwendungen Lichtbilder und Videos in einer Form zusammengeführt und analysiert werden können, die einen schnellen und wirkungsvollen Abgleich ermöglicht (so S. 238 der Begründung des Entwurfes). Diese automatisierte Massenauswertung potenziert die Eingriffsintensität erheblich, auch wegen ihrer Fehleranfälligkeit und des Diskriminierungspotentials.

Die Regelung betrifft ein Hochrisiko-KI-System im Sinne der KI-Verordnung (EU) 2024/1689. Als Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2 i.V.m. Nr. 1 Buchst. a Anhang III der VO gelten jedenfalls biometrische Fernidentifizierungssysteme. Die biometrische Fernidentifizierung ist in Artikel 3 Nummer 41 der KI-Verordnung legaldefiniert: wenn ein KI-System eingesetzt wird, um natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich ihrer biometrischen Daten mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren. Diese Einstufung bringt komplexe Verpflichtungen im Rahmen des Risikomanagements und der Qualitätssicherung, der Transparenz und der Dokumentation mit sich.

Die KI-Verordnung verbietet dabei in Art. 5 Abs. 1 UAbs. 1 lit. e nur das „ungezielte“ Auslesen von Gesichtsbildern aus dem Internet, wodurch nach den Leitlinien der Kommission gezielte Suchen nach Gesichtsbildern von Einzelpersonen oder konkreten Tatverdächtigen grundsätzlich zulässig bleiben sollen (Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz vom 29. Juli 2025, C(2025) 884 final, Rn. 228 f.). § 28a Abs. 1 Satz 3 erlaubt, allgemein zugängliche personenbezogene Daten aus dem Internet zu diesem Zweck zu erheben, zu speichern und aufzubereiten, ohne jedoch eine unverzügliche Löschung nach Zweckerreichung anzuordnen.
Zielrichtung und Art des biometrischen Abgleichs bleiben in der Vorschrift unklar. Der Begriff „Abgleich“ kann sehr verschiedene Verarbeitungsvorgänge umfassen - von der Rasterfahndung über den Abgleich verschiedener Datenmengen miteinander bis hin zur Ermittlung der Identität oder des Aufenthalts (nur in Abs. 1 Satz 1 Nr. 1 berücksichtigt). Diese unterschiedlichen Maßnahmenarten haben jedoch völlig verschiedene Eingriffsintensitäten und erfordern differenzierte rechtliche Anforderungen (vgl. auch BVerfG, Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 120 f.). Da die konkrete Maßnahmenart nicht festgelegt ist, kann die datenschutzrechtliche Erforderlichkeit kaum sachgerecht geprüft werden. Die Schwere des Eingriffs hängt dabei von mehreren Faktoren ab, wie der Art der ausgewerteten Daten, der verwendeten Technologie und dem Automatisierungsgrad. Das verfassungsrechtliche Bestimmtheitsgebot verlangt allerdings, das präzise Regelungen für jeden Grundrechtseingriff getroffen werden. Der Einsatz solcher Systeme im öffentlichen Raum sowie die heimliche Identifizierung von Personen und die anlasslose Erfassung zahlreicher Unbeteiligter verschärft den Eingriff (vgl. auch die Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. September 2024 zum Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden).

Darüber hinaus ist zu berücksichtigen, dass die nachträgliche Fernidentifizierung je nach Einsatzzweck eingriffsintensiver sein kann als Echtzeit-Überwachung: „Wird Videomaterial in Echtzeit durchsucht, kann die Strafverfolgungsbehörde nur herausfinden, wo sich der Verdächtige aktuell aufhält […]; scannt sie dagegen Videos der vergangenen Tage, Wochen oder Monate – also nachträglich –, kann sie ein ganzes Bewegungs- oder Persönlichkeitsprofil erstellen“ (Hahn, ZfDR 2023, 142, 156). Diese differenzierte Eingriffsanalyse fehlt zu § 28a vollständig.

Problematisch ist zudem die hohe Fehleranfälligkeit entsprechender Systeme. Selbst bei einer außerordentlich geringen Fehlerquote wäre aufgrund der großen Menge an erfassten Personen die Zahl der zu Unrecht Betroffenen sehr hoch (so auch Hahn, ZfDR 2023, 142, 168). Dies führt dazu, dass Personen aufgrund von automatisierten Falschbewertungen zu Unrecht eingriffsstarken polizeilichen Maßnahmen unterworfen werden können.

Die Diskriminierungsrisiken sind dabei empirisch belegt, insbesondere eine deutlich höhere Falschakzeptanzrate bei Menschen mit asiatischem Aussehen sowie bei Schwarzen (Ogorek, LTZ 2024, 274, 280, unter Verweis auf Grother/Ngan/Hanaoka (NIST), Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, Dezember 2019, S. 2). Solche systematischen Verzerrungen verstärken das verfassungsrechtliche Problem erheblich. Um den Vorgaben des Art. 3 Abs. 3 GG gerecht zu werden, muss die im Entwurf nicht näher spezifizierte „automatisierte Anwendung zur Datenverarbeitung“ unter Berücksichtigung dieser Erkenntnisse entwickelt werden.

Der in § 28a Abs. 2 Satz 1 enthaltene Verweis auf § 42a Abs. 2 und 3 zeigt konzeptionelle Schwächen der Regelung auf. § 42a regelt die Zweckbindung und den Grundsatz der hypothetischen Datenneuerhebung. Absatz 2 konkretisiert die Anforderungen an eine zweckändernde Weiterverarbeitung personenbezogener Daten und verlangt, dass die neue Nutzung dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Absatz 3 verschärft diese Anforderungen für Daten, die durch besonders eingriffsintensive Maßnahmen wie verdeckte Eingriffe in Wohnungen oder informationstechnische Systeme erlangt wurden: Hier ist zusätzlich erforderlich, dass im Einzelfall die jeweilige Gefahrenschwelle im Sinne von § 25b Abs. 1 (gegenwärtige Gefahr) beziehungsweise § 26b Abs. 1 (konkretisierte Gefahr bei terroristischen oder organisierten Straftaten) erreicht ist. Dieser Verweis macht deutlich, dass die Polizei für den biometrischen Abgleich auch auf Daten aus hochinvasiven verdeckten Maßnahmen zugreifen will. Dies potenziert die Eingriffsintensität erheblich und zeigt, dass § 28a nicht als isolierte Maßnahme konzipiert ist, sondern als Instrument zur Verwertung sensibler Datenbestände genutzt werden kann.

Zu der in § 28a Abs. 5 vorgesehenen Regelung durch Verwaltungsvorschriften gilt das zu § 42d Abs. 4 Gesagte entsprechend.

Die vorgesehenen Kontrollmechanismen erweisen sich als unzureichend. Zwar ist in § 28a Abs. 4 Satz 2 vorgesehen, dass der behördliche Datenschutzbeauftragte nach jeder Maßnahme zu unterrichten ist, jedoch ersetzt dies nicht die vom Bundesverfassungsgericht geforderte verpflichtende regelmäßige und unabhängige Kontrolle. Zum nachträglichen Einsatz des behördlichen Datenschutzbeauftragten als kompensatorische Maßnahme zu einem heimlichen, intensiven Grundrechtseingriff gilt, dass der behördliche Datenschutzbeauftragte als interne Kontrollinstanz strukturell nicht geeignet ist, die erforderliche unabhängige Kontrolle bei derart eingriffsintensiven Maßnahmen zu gewährleisten. Ein systematisches Monitoring der eingesetzten Software ist nicht vorgeschrieben, und es mangelt an wirksamen Vorkehrungen gegen die spezifische Fehleranfälligkeit komplexer KI-Systeme.

Das Fehlen von Benachrichtigungspflichten verstärkt das bereits erhebliche Rechtsschutzdefizit (s. auch Ogorek, LTZ 2024, 274, 278 f.).

Ich empfehle die vollständige Streichung des § 28a.

§ 42 Allgemeine Befugnisse für die Datenweiterverarbeitung

Der Entwurf führt in Absatz 2 eine Legaldefinition für die Weiterverarbeitung ein, die als Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, der Abgleich oder die Verknüpfung von Daten definiert wird. Nach der Begründung orientiert sich diese Definition an der entsprechenden Begrifflichkeit im Bundeskriminalamtgesetz (vgl. S. 270 der Begründung des Entwurfes).

Die Verwendung des Begriffes „Weiterverarbeitung“ ist jedoch problematisch, da dieser Begriff im modernen Datenschutzrecht vorwiegend im Kontext der zweckändernden Verarbeitung genutzt wird. So definiert § 4 Absatz 3 BDSG Weiterverarbeitung als zweckändernde Verarbeitung, ebenso verwenden Erwägungsgrund Nr. 47 Satz 4 DSGVO und Erwägungsgrund Nr. 11 Satz 4 JI-RL den Begriff in diesem Sinne. Dieser terminologische Widerspruch führt zu rechtlicher Unsicherheit und erschwert die einheitliche Anwendung der unionsrechtlichen und nationalen Datenschutzbestimmungen.

Absatz 4 erlaubt die Weiterverarbeitung personenbezogener Daten zur vorbeugenden Bekämpfung von Straftaten und verweist dabei auf die in der Begründung genannten sechs Personenkategorien (vgl. S. 131 der Begründung des Entwurfes). Diese umfassen

u.a. Personen, „bei denen aufgrund tatsächlicher Anhaltspunkte eine hinreichende Wahrscheinlichkeit dafür besteht, dass sie eine strafrechtlich relevante Verbindung zu Straftaten aufweisen werden." Diese Formulierung verstößt gegen die vom Bundesverfassungsgericht entwickelten Grundsätze: „Der konkrete Ermittlungsansatz [...] ist ein einzelfallbezogener tatsächlicher Anlass, der sich aus den Daten selbst oder in Verbindung mit weiteren Erkenntnissen der Behörde ergeben muss. [...] Allgemeine kriminologische Erwägungen oder Erfahrungssätze reichen daher für sich genommen nicht aus. Vielmehr müssen sich aus den Informationen zureichende tatsächliche Anhaltspunkte für eine Straftatenbegehung oder -aufdeckung ergeben" (BVerfG, Urteil vom 1. Oktober 2024 - 1 BvR 1160/19, Rn. 139). Der in Absatz 4 ermöglichte präventive Ansatz verstößt gegen das Verbot der Überwachung „ins Blaue hinein".

§ 42a Zweckbindung und Grundsatz der hypothetischen Datenneuerhebung

§ 42a regelt die datenschutzrechtlichen Grundsätze der Zweckbindung und der sogenannten hypothetischen Datenneuerhebung (HyDaNe) für Ordnungsbehörden und Polizei neu. Die Norm soll die Vorgaben des Bundesverfassungsgerichts aus dem BKAG-Urteil von 2016 umsetzen.

Absatz 1: Zweckwahrende Weiterverarbeitung

§ 42a Abs. 1 soll die Weiterverarbeitung personenbezogener Daten innerhalb der ursprünglichen Zweckbindung regeln. Dies ist nicht durchgängig geglückt. Nach der Vorschrift liegt eine erlaubte zweckwahrende Weiterverarbeitung vor, wenn eine der drei Nummern erfüllt ist.

Nummer 1: Die Weiterverarbeitung muss „zur Erfüllung derselben Aufgabe" erfolgen. Da die Aufgabenzuweisung im ASOG oft nicht trennscharf zwischen den Zwecken der Gefahrenabwehr, der Verhütung von Straftaten und der Strafverfolgungsvorsorge unterscheidet, die in der Praxis fließend ineinander übergehen, ohne dass die jeweilige Ermächtigungsgrundlage stets eine klare Zielrichtung erkennen lässt, kann es hier zu Rechtsunsicherheiten kommen.

Nummer 2: Die Begrenzung auf den Schutz „derjenigen Rechtsgüter oder sonstigen Rechte, den die [ursprüngliche] Ermächtigungsgrundlage bezweckt" weist eine Erweiterung gegenüber dem bundesrechtlichen Vorbild auf. § 12 Abs. 1 BKAG etwa erlaubt die Weiterverarbeitung präziser nur „zum Schutz derselben Rechtsgüter". Der Berliner Entwurf

erweitert dies zudem durch den unbestimmten Begriff „sonstige Rechte“. In der Begründung wird dies nicht weiter erläutert. Während „Rechtsgüter“ ein etablierter strafrechtlicher und verfassungsrechtlicher Begriff mit klaren Konturen ist (Leben, Gesundheit, Eigentum etc.), sind „sonstige Rechte“ völlig unbestimmt. Diese Formulierung kann praktisch jede subjektive Rechtposition umfassen - von Persönlichkeitsrechten über vermögensrechtliche Ansprüche bis hin zu verwaltungsrechtlichen Positionen. Die Rechtsprechung des Bundesverfassungsgerichts verlangt, dass sich die Zweckbindung „nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage“ bestimmt (BVerfG, Urteil vom 1. Oktober 2024 - 1 BvR 1160/19, Rn. 134). Die hier verwendete Formulierung macht eine konkrete Bestimmung nur schwer möglich und eröffnet eine sehr weite Auslegung des Verwendungszwecks.

Nummer 3: Die Formulierung, die Zweckbindung bleibe bestehen „zur vorbeugenden Bekämpfung solcher Straftaten [...], deren Verfolgung [...] die [ursprüngliche] Ermächtigungsgrundlage bezweckt“ kann nicht gefolgt werden. Wenn Daten, die ursprünglich zur Strafverfolgung erhoben wurden, nunmehr für die vorbeugende Bekämpfung von Straftaten verwendet werden, liegt eine Zweckänderung vor. Eine solche Verwendung fällt daher nicht unter Abs. 1 (Zweckbindung), sondern unter Abs. 2 (Zweckänderung) und müsste den dort vorgesehenen Voraussetzungen genügen.

Die Vorschrift erlaubt damit mehr als nur die weitere Nutzung im Rahmen der ursprünglichen Zwecke. Das Bundesverfassungsgericht verlangt gerade, die Zweckbindung nicht allein an abstrakt definierten Behördenaufgaben zu messen, sondern an der Reichweite der Erhebungszwecke in der maßgeblichen Ermächtigungsgrundlage (Urteil vom 20. April 2016- 1 BvR 966/09, 1 BvR 1140/09, Rn. 278f.).

Absatz 2: Zweckändernde Weiterverarbeitung
§ 42a Abs. 2 soll insbesondere das Kriterium der hypothetischen Datenneuerhebung regeln, das zur Prüfung einer zweckändernden Weiterverarbeitung in der Rechtsprechung des Bundesverfassungsgerichts als eingrenzendes Instrument der verfassungsrechtlichen Verhältnismäßigkeitsprüfung entwickelt wurde (vgl. Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 286 ff.). Das Bundesverfassungsgericht entwickelt damit einen offenen verfassungsgerichtlichen Prüfungsmaßstab, nicht ein normatives Programm zur Erstellung einer Befugnisnorm.

Bewertung der einzelnen Voraussetzungen:
Nummer 1 a) – Strafverfolgung: § 481 Abs. 1 Satz 1 StPO erlaubt als generelle Öffnungsklausel eine Verwendung personenbezogener Daten für polizeiliche Zwecke nach Maßgabe der Polizeigesetze. Die hier vorgesehene Einschränkung zur Verfolgung von Straftaten von vergleichbarem Gewicht ist geeignet, die Außerkraftsetzung des Zweckbindungsgebots in § 481 Abs. 1 Satz 1 StPO einzuschränken. In Anbetracht der Tatsache, dass durch die Umwidmung jedoch ein erneuter Eingriff in das Grundrecht auf informationelle Selbstbestimmung erfolgt, sollte eine Verwendung nur restriktiv zugelassen werden, etwa zum Schutz elementarer Rechtsgüter (BeckOK StPO/Wittig StPO § 481 Rn. 2.1 m.w.N.). Die Umwidmung muss insbesondere dem Grundsatz der Verhältnismäßigkeit genügen und daher für die Erreichung des präventiv-polizeilichen Zwecks erforderlich sein (MüKoStPO/Singelnstein StPO § 481 Rn. 8), was normiert werden sollte.

Nummer 1 b) – Gefahrenabwehr: Der Begriff „mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte“ ist unbestimmt und zu weit. Es fehlt an einer präzisen Bestimmung der Schutzgüter, die eine zweckändernde Verarbeitung rechtfertigen können.

Wir begrüßen aber die ausdrückliche Regelung des konkreten Ermittlungsansatzes in Abs. 2 Satz 1 Nr. 2 (s. BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19, Rn. 144).

Der Ausschluss der allgemeinen Datenschutzbestimmungen in Abs. 2 Satz 6 ist teilweise zu begrüßen. Der Ausschluss von § 34 BlnDSG ist sachgerecht, da diese Vorschrift nach aktueller Rechtsprechung zu weite Zweckänderungen zulässt. Problematisch ist jedoch der Ausschluss von § 15 Abs. 5 BlnDSG, der teilweise schärfere Anforderungen an die zweckändernde Verarbeitung besonderer Datenkategorien stellt.

§ 42a Abs. 3 enthält verschärfte Anforderungen für die Weiterverarbeitung von Daten aus besonders eingriffsintensiven verdeckten Maßnahmen (verdeckter Einsatz technischer Mittel in Wohnungen und für Online-Durchsuchungen). Für diese Daten muss zusätzlich die ursprüngliche Gefahrenschwelle weiterhin vorliegen. Die Regelung entspricht den verfassungsrechtlichen Mindestvorgaben, wonach für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen jede weitere Nutzung die Erfüllung aller Eingriffsvoraussetzungen wie bei der Datenerhebung selbst erfordert (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09, Rn. 283).

Die Regelung des Abs. 4 erscheint eher überflüssig, da letztlich für alle gesetzlichen Anforderungen gilt, dass diese technisch-organisatorisch abzusichern sind (§ 57 BlnDSG).

§ 42b: Kennzeichnung

Der neue § 42b führt erstmalig eine umfassende Kennzeichnungspflicht für personenbezogene Daten bei der Speicherung in polizeilichen und ordnungsbehördlichen Informationssystemen ein. Die Regelung soll die vom Bundesverfassungsgericht im BKAG-Urteil von 2016 geforderte praktische Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung ermöglichen.

Die Kennzeichnungspflicht nach Absatz 1 verpflichtet zur Angabe des Erhebungsmittels (einschließlich der Information über offene oder verdeckte Erhebungen), der Personenkategorie, der durch die Erhebungsvorschrift geschützten Rechtsgüter oder zu verhütenden Straftaten sowie der erhebenden Stelle. Nach der Begründung des Entwurfs soll diese Kennzeichnung „die Voraussetzung für eine umfassende Anwendung des Grundsatzes der hypothetischen Datenneuerhebung“ schaffen (vgl. S. 281 der Begründung des Entwurfs). Die Kennzeichnung kann optional durch Angabe der Rechtsgrundlage ergänzt werden und erfasst auch personenbezogene Daten, denen keine Erhebung vorausgegangen ist.

Absatz 2 verpflichtet empfangende Stellen zur Aufrechterhaltung der Kennzeichnung nach Datenübermittlungen. Dies entspricht unserem in früheren Stellungnahmen geäußerten Grundverständnis, dass die Zweckbindung auch bei der Weiterverarbeitung durch andere Stellen gewahrt bleiben muss.

Problematisch ist allerdings die in Absatz 3 vorgesehenen Ausnahmen von der Kennzeichnungspflicht. Nach Nummer 1 entfällt die Kennzeichnungspflicht bei tatsächlicher Unmöglichkeit, nach Nummer 2 auch bei technischer Unmöglichkeit oder unverhältnismäßigem technischen Aufwand. Letztere Ausnahme soll nach der Begründung „nur befristet Anwendung finden“ und am 1. Januar 2031 entfallen (vgl. S. 283 der Begründung des Entwurfs). Die Frist wird laut Bergründung für erforderlich, aber auch für ausreichend erachtet, damit die Polizei Berlin die Kennzeichnungspflicht in ihren Informationssystemen umsetzen kann.

Die in § 42b Absatz 3 beabsichtigte Regelung wäre akzeptabel, wenn ausdrücklich geregelt wird, dass nur gekennzeichnete Daten zweckändernd verwendet werden dürfen. Das

Bundesverfassungsgericht fordert „hinreichend normenklare Regelungen [...], die die Einhaltung des Grundsatzes der Zweckbindung rechtlich und praktisch sichern“ (BVerfG, Urt. v. 16. Februar 20-3 - 1 BvR 1547/19 u.a., Rn. 65). Die Prüfung der Voraussetzungen der hypothetischen Datenneuerhebung erfordert eine vorherige Kennzeichnung der Daten. Solange die Berliner Polizei die technischen Voraussetzungen zur Kennzeichnung schafft, kann sie das Instrument der hypothetischen Datenneuerhebung nicht gemäß den Vorgaben des Bundesverfassungsgerichts in der Breite anwenden. Das Grundrecht auf informationelle Selbstbestimmung verlangt, dass staatliche Datenverarbeitung von vornherein so strukturiert wird, dass verfassungsrechtliche Grenzen eingehalten werden können.

Ich empfehle eine klarstellende Regelung entsprechend § 14 Absatz 2 BKAG, nach der nur ordnungsgemäß gekennzeichnete Daten für zweckändernde Weiterverarbeitungen verwendet werden dürfen. Alternativ sollte die Ausnahmeregelung in Absatz 3 Nummer 2 gestrichen und die technische Unmöglichkeit nur in absoluten Ausnahmefällen anerkannt werden.

Ergänzend rege ich an, die Kennzeichnungspflicht um eine weitere Nummer zu erweitern: „Zeitpunkt, zu dem die Daten von der erhebenden Stelle gelöscht werden oder die Löschung zu prüfen ist“. Diese Information ist gerade bei Datenübermittlungen zur Überprüfung der Rechtmäßigkeit für die empfangende Stelle wichtig und kann die Einhaltung von Löschfristen unterstützen.

Bei der Kennzeichnung besonderer Kategorien personenbezogener Daten sollten zusätzliche Garantien für die Rechte und Freiheiten betroffener Personen eingeführt werden. Besondere Kategorien personenbezogener Daten sollten zu diesem Zweck gesondert gekennzeichnet werden, um dem erhöhten Schutzbedarf dieser Daten Rechnung zu tragen.

§ 42d: Training und Testung von KI-Systemen

Der neue § 42d schafft eine spezifische Rechtsgrundlage für Polizei und Feuerwehr, rechtmäßig gespeicherte personenbezogene Daten über die vorgesehene Speicherdauer hinaus zum Training und zur Testung von KI-Systemen zu verarbeiten, die der Erfüllung ihrer jeweiligen Aufgaben dienen. Die Neuregelung ermöglicht die zweckändernde Weiterverarbeitung sämtlicher rechtmäßig gespeicherter personenbezogener Daten nach einem gestuften Verfahren, das vorrangig Anonymisierung, hilfsweise Pseudonymisierung

und ausnahmsweise auch die Verarbeitung von nicht-pseudonymisierten personenbezogenen Daten vorsieht. Lediglich personenbezogene Daten aus den in § 42c Absatz 2 genannten besonders eingriffsintensiven Maßnahmen sind von der Weiterverarbeitung ausgenommen (medizinische und körperliche Untersuchungen, offene und verdeckte Aufzeichnungen in privaten Räumen sowie heimliche IT-Systemeingriffe).

Im Anwendungsbereich der Polizei verstößt die Regelung gegen Grundprinzipien der JI-Richtlinie (Richtlinie (EU) 2016/680). Art. 8 Abs. 1 JI-RL verpflichtet die Mitgliedstaaten zur Implementierung eines Verarbeitungsverbots mit Erlaubnisvorbehalt. § 42d Absatz 1 formuliert hingegen eine pauschale Ermächtigung ohne ausreichende Begrenzungen. Art. 10 JI-RL fordert für besondere Kategorien personenbezogener Daten eine unbedingte Erforderlichkeit und geeignete Garantien. Der Verweis auf § 51a Absatz 2 in Abs. 2 Satz 4 genügt diesen Anforderungen nicht. Art. 7 JI-RL verpflichtet zudem zur Unterscheidung zwischen faktenbasierten Daten und persönlichen Einschätzungen. Art. 6 JI-RL verpflichtet zur Differenzierung verschiedener Betroffenenkategorien. Vorliegend sind diese gesetzlichen Anforderungen in der Norm nicht adressiert. Auch die Daten Unbeteiligter ist von der zweckändernden Weiterverarbeitung nicht ausgeschlossen.

Die KI-Verordnung (EU) 2024/1689 enthält in Artikel 5 absolute Verbote bestimmter KI-Praktiken, insbesondere für Social Scoring-Systeme und biometrische Kategorisierungssysteme, und verschiedene Risikoklassen. Diese sollten sich in § 42d in Form einer Konkretsierung im Kontext des Polizei- und Gefahrenabwehrrechts wiederspiegeln.
Die in § 42d Absatz 1 Satz 1 vorgesehene Möglichkeit, personenbezogene Daten über die vorgesehene Speicherdauer hinaus zu verarbeiten, durchbricht das fundamentale Prinzip der Zweckbindung und untergräbt verfassungsrechtlich gebotene Löschpflichten. Die ursprünglich gesetzten Speicherfristen sind bewusst normiert, um das Recht auf informationelle Selbstbestimmung zu schützen. Die unbegrenzte Verlängerung der Speicherdauer für einen völlig anderen Zweck stellt einen neuen, eigenständigen Grundrechtseingriff dar, der einer gesonderten verfassungsrechtlichen Rechtfertigung bedürfte. Zudem ist vollkommen unklar, wie zum Training genutzte Daten, die zwischenzeitlich gelöscht werden müssten, aus einem KI-Modell entfernt werden sollen.

Die Ziele des Trainings und die Art der zu entwickelnden KI-Systeme bzw. mögliche Einsatzzenarien werden nicht spezifiziert. § 42d Absatz 1 Satz 1 beschränkt sich auf die Aus-

sage, dass die KI-Systeme „der Erfüllung ihrer jeweiligen Aufgaben dienen“. Diese Formulierung ist derart weit gefasst, dass sie praktisch jede denkbare KI-Anwendung erfasst. Zudem ist das Verhältnis zu § 42 und 42a vollkommen unklar. So scheint es, dass § 42d eine eigene Weiterverwendungsregel darstellt. Die zweckändernde Verarbeitung von personenbezogenen Daten ist aber an weitere verfassungsrechtliche Vorgaben gebunden, die in der Norm nicht abgebildet sind. Sofern der spätere Einsatz eines KI-Modells bzw. -System zum Schutze anderer Rechtsgüter erfolgt als die Erhebung der Daten, muss die Weiterverwendung dieser Daten den verfassungsrechtlichen Grundsätzen der hypothetischen Datenneuerhebung genügen. Selbst wenn ein KI-Einsatzszenario zum jetzigen Zeitpunkt nicht hinreichend konkret beschrieben werden kann, so müsste die zweckändernde Nutzung in der Norm dennoch so eingehegt werden, dass zum Zeitpunkt des Trainings gewährleistet wird, dass die zum Training verwendeten Daten nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln neu erhoben hätten werden dürfen. Diese Anforderung muss in der Norm selbst sichergestellt werden. Die Norm genügt damit nicht dem verfassungsrechtlichen Bestimmtheitsanforderungen.

Das in § 42d Absatz 2 vorgesehene gestufte Schutzkonzept halten wir in dieser Pauschalität als Schutzkonzept für unrealistisch. Die Begründung geht davon aus, dass „vorrangig anonymisierte, d.h. nicht personenbezogene, Daten zu verwenden“ sind (vgl. S. 289 der Begründung des Entwurfes). In der Praxis ist jedoch eine wirksame Anonymisierung komplexer Datensätze, insbesondere bei biometrischen oder Verhaltensdaten, regelmäßig sehr aufwändig bis unmöglich. Die Regelung läuft daher auf eine systematische Verwendung von Klardaten hinaus.

Die Übermittlungsmöglichkeiten an private Dritte nach § 42d Absatz 3 sind verfassungsrechtlich bedenklich. Insbesondere die in Absatz 3 Satz 8 vorgesehene Möglichkeit der Weiternutzung trainierter Modelle mit Genehmigung der Polizei bzw. Feuerwehr schafft Risiken für die Zweckbindung der ursprünglich erhobenen Daten. Als einzige Voraussetzung für die Übermittlung personenbezogener Daten an Dritte sieht die Vorschrift vor, dass die Verarbeitung den Verantwortlichen selbst auch unter Zuhilfenahme von Auftragsverarbeitern nicht oder nur unter unverhältnismäßigem Aufwand möglich ist. Insbesondere das letztgenannte Kriterium ist kein ausreichendes oder bestimmtes Kriterium für die Weitergabe polizeilicher Daten an Dritte, da es eine rein wirtschaftliche Abwägung ermöglicht, bei der Kostenaspekte über das erforderliche Schutzniveau gestellt werden können, und

damit den Verhältnismäßigkeitsmaßstab für eingriffsintensive Datenverarbeitungen durch eine unbestimmte, in der Praxis vernachlässigbare Hürde ersetzt.

Ob die in § 42d Absatz 4 vorgesehene Umsetzung durch Verwaltungsvorschriften mit der Wesentlichkeitstheorie vereinbar ist, ist zweifelhaft. Wesentliche Entscheidungen wie Löschfristen, konkrete Trainingsmethoden, zulässige KI-Systemtypen oder spezifische Schutzmaßnahmen müssen bereits im Gesetz geregelt werden. Soweit Näheres zum Verfahren in einer Verwaltungsvorschrift zu bestimmen ist, dürfte darunter zentral die Vorgehensweise bei der Weiterverarbeitung fallen. Der Vorschrift kann nicht entnommen werden, welches Verfahren zur Verarbeitung von personenbezogenen Daten beim Testen und Trainieren tatsächlich durch die Polizei und die Feuerwehr (und ihre Auftragsdatenverarbeiter) eingesetzt wird. Um überhaupt eine Verwaltungspraxis vorzugeben, wird daher empfohlen, das Verfahren für die Adressaten detaillierter darzulegen, soweit dies aus Sicherheitsgründen möglich ist. Dies beinhaltet die Beschreibung, welche Prozesse die zunächst von der Polizei erhobenen personenbezogenen Daten beim Auftragsdatenverarbeiter durchlaufen und in welcher Form die so generierten personenbezogenen Daten weiterverarbeitet werden.

Die Regelung zum KI Training bedarf einer umfassenden Überarbeitung.

§ 43: Allgemeine Grundsätze der Datenübermittlung

Der neue § 43 führt erstmals allgemeine Grundsätze und Begrenzungen ein, die bei allen Datenübermittlungen nach dem ASOG zu beachten sind. Damit soll klargestellt werden, dass die Grundsätze der Datenübermittlung für alle entsprechenden Vorgänge nach dem Gesetz gelten. Zentral ist dabei die Verweisung auf § 42a Absatz 2 bis 4, wodurch der Grundsatz der hypothetischen Datenneuerhebung auch für Datenübermittlungen verbindlich wird (vgl. S. 292 der Begründung des Entwurfes). Die Begründung führt richtigerweise aus, dass „die Datenübermittlung eine zweckändernde Form der Weiterverarbeitung von Daten ist," so dass „die vom Bundesverfassungsgericht im BKAG-Urteil von 2016 aufgestellten Anforderungen an die Zweckänderung umzusetzen" sind (vgl. S. 292 f. der Begründung des Entwurfes). § 43 soll dabei die allgemeinen Regelungen des Berliner Datenschutzgesetzes verdrängen.

Die Einführung dieser übergreifenden Regelung ist aus datenschutzrechtlicher Sicht grundsätzlich zu begrüßen, da sie die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts zur hypothetischen Datenneuerhebung systematisch in das Gesetz einbindet.

§ 45 Abs. 2 bis 6: Datenübermittlung an proaktive Beratungsstellen

§45 schafft in den Absätzen 2 bis 6 erstmals eine spezifische Rechtsgrundlage für die Übermittlung von Kontaktdaten von volljährigen Opfern und Tätern bestimmter Rechtsgutverletzungen an geeignete Beratungs- oder Vermittlungsstellen nach einer Interessensabwägung. Mit Einwilligung der betroffenen Person können ihre Daten auch stets außerhalb dieser Vorgaben übermittelt werden.

Ein Zustimmungserfordernis sehen wir für alle Arten von Übermittlungen als vorteilhaft an, da auch die Begründung nicht dazu Stellung nimmt, inwiefern eine Übermittlung gegen den Willen der betroffenen Person der Zweckerreichung zuträglich ist. Wir empfehlen zudem eine Evaluation der Wirksamkeit insbesondere bei Übermittlungen ohne Einwilligung.

Die übermittelten Daten sind von der Beratungsstelle zu löschen, wenn die betroffene Person das Angebot ablehnt oder drei Monate lang unbeantwortet lässt. Die Ablehnung des Angebots ist der Polizei unverzüglich mitzuteilen. Dadurch erfährt die Polizei in der Regel, ob die betroffene Person das vertrauliche Beratungsangebot angenommen hat. Hier fehlt es einer strengen Zweckbindung und kurzen Löschsfristen auf Normebene, denn eine zweckändernde Verwendung dieser Information - etwa im Strafverfahren - muss wirksam ausgeschlossen werden, sicherzugehen, dass die Selbstbelastungsfreiheit nicht unterlaufen wird. Ansonsten stände die Freiwilligkeit als auch die Vertraulichkeit der Nutzung dieses Hilfeangebotes in Frage.

§ 47a Automatisierte Anwendung zur Analyse vorhandener Daten

Der neue § 47a schafft erstmals eine gesetzliche Grundlage für die automatisierte Datenanalyse durch die Berliner Polizei. Die Vorschrift ermöglicht es, bisher unverbundene Dateien und Datenquellen in Analyseplattformen zusammenzuführen, zu verknüpfen und aufzubereiten, ohne diese Begriffe näher zu erläutern oder einzugrenzen. Jedenfalls finden sich diese Begrifflichkeiten mit Ausnahme der Verknüpfung auch nicht in den Datenschutzgesetzen von DSGVO, JI-Richtlinie und BlnDSG bisher nicht. Unklar bleibt in diesem Zusammenhang insbesondere die Anwendung für „statistische Zwecke“ (§ 47a Abs. 1 Satz

2) als Teil der automatisierten Datenanalyse. Die vorgeschlagene Regelung wirft nach den Vorgaben des Bundesverfassungsgerichts vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) zur automatisierten Datenanalyse verfassungsrechtliche Fragestellungen auf.

Die Begründung führt aus, dass sich der Entwurf an den nach dem Bundesverfassungsgerichtsurteil überarbeiteten Bestimmungen in Hessen (§ 25a HSOG) und Hamburg (§ 49 PolDVG) orientiert (vgl. S. 331 der Begründung des Entwurfes). Trotz dieser Orientierung entsprechen die vorgesehenen Eingriffsschwellen nicht den verfassungsrechtlichen Anforderungen. Zunächst ist festzustellen, dass § 47a Abs. 1 Satz 1 die voraussetzungslose Zusammenführung gespeicherter personenbezogener Daten nach § 47a Abs. 2 Satz 1 erlaubt. Erst wenn in einem weiteren Schritt nach § 47a Abs. 1 Satz 2 die zusammengeführten Daten im Rahmen der automatisierten Datenanalyse verarbeitet werden, müssen die Voraussetzungen der Eingriffsschwellen nach § 47a Abs. 1 Satz 2 gegeben sein. Bereits die Zusammenführung, Verknüpfung und Aufbereitung stellt aber eine zweckändernde Verarbeitung dar, die unter den Vorbehalt von Eingriffsschwellen zu stellen ist. So ist dies auch in den Bestimmungen in Hessen und Hamburg vorgesehen. Hieran knüpfen sich auch Folgeprobleme an:
Die Verweisung auf § 42a Absatz 1 bis 4, § 42b und § 42c Absatz 1 in § 47a Absatz 2 Satz 6 führt zwar zur Anwendung der Regelungen über zweckwahrende und zweckändernde Datenverarbeitung (§ 42a), der Kennzeichnungspflichten (§ 42b) und der Übermittlungsregelungen zu Forschungszwecken (§ 42c Absatz 1). Da § 47a Abs. 2 sich aber nur auf die automatisierte Datenanalyse bezieht (§ 47a Abs. 1 Satz 2) undnicht auf die Zusammenführung in § 47a Abs. 1 Satz 1, gelten diese – nach Begründung – „zentralen Steuerungsinstrumente“ der zweckwahrenden und zweckändernden Datenverarbeitung nicht bereits für die zweckändernde Zusammenführung. Dies ist mit den verfassungsrechtlichen Vorgaben so nicht vereinbar.

Im Hinblick auf die Eingriffsschwelle des § 47a Abs. 1 Nr. 2 verweist der Entwurf in eine derzeit defekte Norm des § 100a Absatz 2 StPO, ohne die im Einzelfall betroffenen Schutzgüter zu benennen. Hier wäre es zu begrüßen, wenn der Landesgesetzgeber – wie schon an mehreren Stellen angemerkt – eigene am Schutzgut orientierte Kataloge entwickelt, die dann auch im Hinblick auf gesetzgeberische Dynamiken des Bundesgesetzgeber wirksam bleiben.

Insbesondere in Bezug auf die Eingriffshürde in Absatz 1 Satz 2 Nummer 3 („wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet“) ist anzumerken, dass sicherzustellen ist, dass die Eingriffsschwelle Voraussetzung für die Zusammenführung bzw. Datenanalyse ist und nicht umgekehrt, d.h. die Eingriffsschwelle darf nicht erst durch die Datenanalyse sozusagen „errechnet“ werden. Dies gilt – wie gesagt – auch bereits für das Zusammenführen der Daten nach § 47a Abs. 1 Satz 1. Insofern bestehen Zweifel, ob die Formulierung in Abs. 1 Satz 2 Nr. 3 ausreichend konkret ist, um Ermittlungen weit im Gefahrenvorfeld oder gar ins Blaue hinein wirksam auszuschließen.

Die in § 47a Abs. 2 Satz 1 benannten Datenkategorien sieht eine Einbeziehung nahezu sämtlicher polizeilich verfügbarer Datenbestände vor. Unklar bleibt, worunter die Datenerhebungen aus den Eingriffsbefugnissen zu fassen sind. Eine wirksame qualitative oder quantitative Begrenzungen erfolgt nicht. Der Ausschluss von Vorgangsdaten Unbeteiligter in Absatz 2 Satz 5 überzeugt im Hinblick auf seine Schutzwirkung nicht, da unklar bleibt, wie die Kategorisierung, Identifizierung, Kennzeichnung und Abtrennung der Datensätze unbeteiligter Personen in der Praxis erfolgen kann. Dies steht im Widerspruch zu der vom Bundesverfassungsgericht geforderten Reduzierung des Eingriffsgewichts durch entsprechende gesetzliche Vorkehrungen (BVerfG, a.a.O., Rn. 72 ff.).

Die Entscheidungen zu den konkreten Rahmenbedingungen, die in § 47a Abs. 2 Satz 7 einem zu erstellenden Konzept vorbehalten sind, müssen bereits in der Norm eine Konkretisierung erfahren, da es sich um wesentliche Entscheidungen handelt, die gesetzlichen Vorkehrungen zur Reduzierung des Eingriffsgewichts ausprägen. Dabei wäre z.B. vorzugeben, welche Veranlassungszusammenhänge bzw. welche Grundrechtsrelevanz in Betracht kommt.

Die parlamentarische Kontrolle durch das Abgeordnetenhaus gemäß Absatz 7 und die Anhörung des Berliner Beauftragten für Datenschutz und Informationsfreiheit vor Einrichtung oder wesentlichen Änderungen nach Absatz 5 sind positive Elemente, können jedoch die grundsätzlichen verfassungsrechtlichen Bedenken der Regelung nicht kompensieren.

Die Vorschrift bedarf der Überarbeitung.

§ 51b: Datenschutzkontrolle

§ 51b ist eine neue Vorschrift, die spezielle Datenschutzkontrollbefugnisse der Berliner Beauftragten für Datenschutz und Informationsfreiheit bei eingriffsintensiven verdeckten Datenerhebungsmaßnahmen und Datenübermittlungen in Drittstaaten sammelt.

Die Vorschrift verpflichtet die BlnBDI dazu, spätestens alle zwei Jahre Kontrollen bezüglich der Verarbeitung personenbezogener Daten bei bestimmten zu protokollierenden Maßnahmen durchzuführen. Dies umfasst ein breites Spektrum besonders eingriffsintensiver verdeckter Datenerhebungen: anlassbezogene automatisierte Kennzeichenfahndung (§ 24d), längerfristige Observation (§ 25), verdeckten Einsatz technischer Mittel außerhalb von Wohnungen (§ 25a), verdeckten Einsatz technischer Mittel in oder aus Wohnungen (§ 25b), Einsatz Verdeckter Ermittler (§ 25c), Telekommunikationsüberwachung (§ 26), Quellen-Telekommunikationsüberwachung (§ 26a), Online-Durchsuchung (§ 26b), Bestandsdatenauskunft (§ 26c), Verkehrs- und Nutzungsdatenerhebung (§ 26d), Funkzellenabfrage (§ 26e), Ausschreibung zur polizeilichen Beobachtung (§ 27), einzelnen Maßnahmen des nachträglichen biometrischen Abgleich (§ 28a) und besondere Formen des Datenabgleichs (§ 47). Es wird außerdem in einen § 28a Absatz 2 Satz 3 verwiesen, der im aktuellen Entwurf nicht existiert.

Viele dieser Befugnisse greifen nicht nur in das Recht auf informationelle Selbstbestimmung ein, sondern betreffen vordringlich andere spezifische Grundrechte wie das Fernmeldegeheimnis nach Art. 10 GG (Telekommunikationsüberwachung, Quellen-Telekommunikationsüberwachung, Verkehrsdatenerhebung), die Unverletzlichkeit der Wohnung nach Art. 13 GG (verdeckter Einsatz technischer Mittel in Wohnungen) oder das IT-System-Grundrecht (Online-Durchsuchung).

Zusätzlich sind Datenübermittlungen nach § 44b (Drittstaaten) und § 45 Absatz 8 zu kontrollieren, die besondere Risiken für das Recht auf informationelle Selbstbestimmung bergen, da in Drittstaaten möglicherweise geringere Datenschutzstandards gelten.

Der Gesetzgeber begründet die Regelung zutreffend damit, dass „eingriffsintensive und regelmäßig verdeckte Überwachungsmaßnahmen sowie Datenübermittlungen in Drittstaaten nur unter einer effektiven datenschutzaufsichtsrechtlichen Kontrolle zugelassen werden können“ (vgl. S. 353 der Begründung des Entwurfes). Diese Vorgabe folgt aus

dem BKAG-Urteil des Bundesverfassungsgerichts (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 141, 340). Das Bundesverfassungsgericht verlangt jedoch nicht nur formelle Kontrollbefugnisse, sondern eine effektive datenschutzaufsichtsrechtliche Kontrolle. Eine bloße Kontrollpflicht ohne wirksame Anschlussbefugnisse wird diesem verfassungsrechtlichen Maßstab nicht gerecht. § 51b normiert zwar die Kontrollpflicht und den Anspruch auf Zugang zu Protokollen und Dokumentationen, schweigt jedoch zu den Reaktionsmöglichkeiten bei festgestellten Rechtsverstößen.

Für eine effektive Kontrolle im Sinne der verfassungsgerichtlichen Rechtsprechung müsste die Datenschutzaufsicht zumindest über angemessene Anordnungsbefugnisse verfügen, um bei festgestellten Verstößen gegen datenschutzrechtliche Bestimmungen wirksam reagieren zu können. Die bloße Feststellung von Rechtsverstößen ohne entsprechende Durchsetzungsmöglichkeiten genügt den verfassungsrechtlichen Anforderungen an eine effektive Kontrolle nicht.

Während § 51b als Umsetzung verfassungsrechtlicher Vorgaben grundsätzlich zu begrüßen ist, bleibt die Regelung unvollständig, da sie keine ausreichenden Anschlussbefugnisse für eine effektive Kontrolle vorsieht. Die Vorschrift sollte daher um entsprechende Durchsetzungsbefugnisse ergänzt werden, um den verfassungsrechtlichen Anforderungen an eine effektive datenschutzaufsichtsrechtliche Kontrolle zu entsprechen.

Ich empfehle daher eine Ergänzung der Vorschrift um angemessene Anordnungs- und Sanktionsbefugnisse der Datenschutzaufsicht bei festgestellten Verstößen gegen datenschutzrechtliche Bestimmungen bei eingriffsintensiven Maßnahmen. Der Gesetzgeber sollte außerdem darauf achten, dass die Arbeit der BlnBDI nicht dazu vorgesehen ist, seinen ausgeweiteten Befugnisse als kompensatorische Maßnahme den Anschein von Grundrechtskonformität zu verleihen. Er hat außerdem darauf zu achten, dass die verpflichtende Wahrnehmung zahlreicher - teils fachfremder - Kontrollaufgaben nicht schon durch ihre reine Anzahl die Unabhängigkeit beeinträchtigt.

§ 20 BlnDSG-E - Videoüberwachung

Bezüglich der Verlängerung der Speicherdauer weisen wir zunächst darauf hin, dass der Entwurf zu § 20 Abs. 3 Satz 3 BlnDSG in der derzeitigen Fassung streng genommen nicht die Speicherdauer regelt, sondern eine Einschränkung der Übermittlungsbefugnis der Videoaufnahmen.

Unabhängig davon können wir bisher nicht nachvollziehen, dass die Verlängerung der Speicherfrist auf 72 Stunden tatsächlich erforderlich ist. Es ist zwar für uns grundsätzlich nachvollziehbar, dass die meisten der genannten Gründe zu einem Beweismittelverlust aufgrund früherer Löschung von Aufnahmen führen können. Entscheidend ist aber, ob dies mittlerweile in einem Ausmaß der Fall ist, dass eine Erhöhung der Speicherfrist erforderlich und im Hinblick auf die Persönlichkeitsrechte der unbescholtenen Fahrgäste angemessen ist. Zumindest größenordnungsweise müsste ein Nachweis erfolgen. Die Polizei hat uns zwar einzelne Fallbeispiele aus der Vergangenheit benannt. Nicht nachvollziehbar ist aber, dass – wie auch in der Begründung – die Praxis die Notwendigkeit der Verlängerung „zeige“, auf unsere Nachfrage aber weder Polizei noch BVG konkrete Zahlen benennen können.