Deutsche Vereinigung für Datenschutz e.V.
Reuterstraße 157
53113 Bonn
https://www.datenschutzverein.de

Bonn, 06.04.2018

Stellungnahme der **Deutschen Vereinigung für Datenschutz e. v. (DVD)** zum **Gesetzentwurf der Staatsregierung** zur **Neuordnung des Bayerischen Polizeirechts** (PAG-Neuordnungsgesetz) vom 30.01.2018, BayLT-Drs. 17/20425

Vorbemerkung

Der Entwurf zur Novellierung des Polizeiaufgabengesetzes (PAG-E) soll, so die Begründung, europäische sowie verfassungsrechtliche Vorgaben, insbesondere aus der Richtlinie (EU) 2016/680 zum Datenschutz bei Polizei und Justiz vom 27.04.2016 (künftig DSRl-JI – Datenschutzrichtlinie Justiz/Inneres), sowie die befugniseinschränkende Rechtsprechung des Bundesverfassungsgerichts (BVerfG), insbesondere die umfassenden Festlegungen zum Bundeskriminalamtsgesetz,[1] umsetzen. Tatsächlich werden bei dieser Gelegenheit viele **neue polizeilichen Befugnisnormen** vorgeschlagen zwecks „dem Stand der Technik entsprechender Ergänzung und noch effektiveren Ausgestaltung“ (S. 1).

Die vorliegende Stellungnahme befasst sich nicht mit sämtlichen geplanten Neuregelungen, sondern greift diejenigen heraus, die aus Sicht der DVD hinsichtlich des Schutzes der informationellen Selbstbestimmung der Menschen **besonders problematisch** sind. Von den Änderungsvorschlägen betroffen ist nicht nur das Grundrecht auf Datenschutz (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Art. 8 GRCh), sondern in Fällen des Zugriffs auf private informationstechnische (IT-) Systeme das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[2], sowie bei vielen Maßnahmen das Telekommunikationsgeheimnis (Art. 10 GG, Art. 7 GRCh), das Recht auf Schutz der Wohnung (Art. 13 GG, Art. 7 GRCh) sowie weitere informationelle Grundrechte.[3]

Nicht näher behandelt werden u. a. folgende neue, auch **verfassungsrechtlich problematische Befugnisnormen**:

- die Möglichkeit einer polizeilichen Meldeanordnung (Art. 16 Abs. 2 Nr. 2 PAG-E),[4]

[1] BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, NJW 2016, 1781 = DuD 2016, 469 = EuGRZ 2016, 149 = DVBl 2016, 770 = K&R 2016, 395 = NVwZ 2016, 839 (LS mit Anm. Wiemers) = CR 2016, 796 (BKA-Gesetz)

[2] BVerfG 27.02.2008 – 1 BvR 370/07 u. 1 BvR 595/07, NJW 2008, 822 = DÖV 2008, 459 = MMR 2008, 315 = DVBl 2008, 411 (Online-Durchsuchung); Weichert in Däubler u. a., Bundesdatenschutzgesetz, 5. Aufl. 2016, Einl. Rn. 13.

[3] Weichert in Däubler u. a. (Fn. 2), Einl. Rn. 30 ff.

[4] Dazu kritisch Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD), Stellungnahme vom 21.12.2017, https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf, S. 7 f.; Löffelmann, Stellungnahme zum PAG-Entwurf eines PAG-Neuordnungsgesetzes vom 14.02.2018, Rn. 11.

- die Herabsenkung der Eingriffsschwelle beim Betreten und Durchsuchen von Wohnungen durch Ersetzen des Begriffs der gegenwärtigen Gefahr durch den der dringenden Gefahr (Art. 23 Abs. 1 Nr. 3 PAG-E),[5]

- die Ausweitung der Befugnisse für Aufgaben der Grenzkontrolle und Sicherung von Anlagen (Art. 29 PAG-E),[6]

- die Ausweitung der Befugnis zur Verarbeitung besonderer Kategorien personenbezogener Daten ohne eine unbedingte Erforderlichkeit oder Grundrechtsgarantien vorzusehen (Art. 30 Abs. 2 PAG-E),[7]

- die Datenerhebung zu Zwecken des Personenschutzes ohne Erfordernis einer Zustimmung des Betroffenen (Art. 32 Abs. 1 S. 1 Nr. 1b, 61 Abs. 1 PAG-E),[8]

- die Erstellung und Aufzeichnung von Bild und Ton bei öffentlichen Veranstaltungen und von Videos bei Anhaltspunkten für Straftaten und erheblichen Ordnungswidrigkeiten sowie von Übersichtsaufnahmen (Art. 33 Abs. 1 PAG-E).[9]

- der Einsatz von sog. Bodycams zum Schutz eines bedeutenden Rechtsguts (Art. 33 Abs. 4 S. 1 PAG-E),[10]

- die Weiterung der erst jüngst eingeführten elektronischen Aufenthaltsüberwachung (Art. 34 PAG-E),[11]

- die Postsicherstellung bei mutmaßlichem Gefahrenbezug auch bei einem Nachrichtenmittler (Art. 35 Abs. 1 PAG-E),[12]

- die Übertragung der Befugnis zur Postöffnung an die Polizei (Art. 35 Abs. 4, 5 PAG-E),[13]

- die Ausweitung der Fristen für den Einsatz verdeckter Ermittler (Art. 37 Abs. 2, 3 PAG-E),[14]

- der Einsatz von Vertrauenspersonen als Standard- und nicht als absolute Ausnahmemaßnahme (Art. 38 Abs. 2 PAG-E),[15]

[5] Dazu kritisch BayLfD (Fn. 4), S. 11 f.; Löffelmann (Fn. 4), Rn. 17.
[6] Dazu kritisch BayLfD (Fn. 4), S. 15 ff.
[7] Dazu kritisch BayLfD (Fn. 4), S. 17 ff.; Löffelmann (Fn. 4), Rn. 24.
[8] Dazu kritisch BayLfD (Fn. 4), S. 20 f., 69 f
[9] Dazu kritisch BayLfD (Fn. 4), S.24; Löffelmann (Fn. 4), Rn. 31; Graulich, Gutachterliche Anmerkungen zu den Gesetzentwürfen der Bayerischen Staatsregierung v. 14.03.2018, S. 17 ff.
[10] Dazu kritisch BayLfD (Fn. 4), S. 25.
[11] Dazu kritisch Löffelmann (Fn. 4) Rn. 35
[12] Dazu kritisch BayLfD (Fn. 4), S. 31 f.; Löffelmann (Fn. 4), Rn. 36.
[13] Dazu kritisch BayLfD (Fn. 4) S. 32.
[14] Dazu kritisch BayLfD (Fn. 4), S. 35; Löffelmann (Fn. 4) Rn. 47, 49.
[15] Dazu kritisch BayLfD (Fn. 4), S. 36 ff.; Löffelmann (Fn. 4) Rn. 47.

- die Ausweitung der Befugnis zur polizeilichen Beobachtung (Art. 40 PAG-E),[16]
- die Ausweitung der Befugnis zur Funkzellenabfrage, ohne aber eine klare Regelung vorzunehmen (Art. 43 PAG-E),[17]
- die Zulassung der Online-Durchsuchung schon bei einer drohenden Gefahr bestimmter Rechtsgüter (Art. 45 PAG-E).[18]
- Dies erfolgt unter
- ungenügendem Schutz von Berufsgeheimnissen sowie des Kernbereichs privater Lebensgestaltung (Art. 49 PAG-E),[19]
- unter ungenügender parlamentarischer sowie öffentlicher Unterrichtung und Kontrolle (Art. 52, 58 Abs. 6 PAG-E),[20]
- ungenügender unabhängiger richterlicher Kontrolle (Art. 53, 92 Abs. 3 PAG-E),[21]
- unter unzureichender Beachtung der verfassungsrechtlich begründeten Löschpflichten (Art. 54 PAG-E)[22] und
- unter übermäßiger Beschränkung des Auskunftsanspruchs von Betroffenen (Art. 65 Abs. 2 PAG-E).[23]

Nicht vertieft behandelt werden hier die geplanten Regelungen zur **DNA-Analyse** (DNA-Identifizierung, DNA-Phänotypisierung, Art. 14 Abs. 3, 32 Abs. 1 S. 2 u. 3 PAG-E). Hierzu wurde vom Netzwerk Datenschutzexpertise eine ausführliche Stellungnahme[24] erarbeitet, die zu dem Ergebnis kommt, dass die geplanten Regelungen gegen europäisches und nationales Verfassungsrecht sowie gegen die europarechtlichen Vorgaben der DSRl-JI verstoßen. Grund für diese Bewertung ist, dass nicht erforderliche und unverhältnismäßige Maßnahmen mit einem hohen Diskriminierungsrisiko erlaubt werden sollen, ohne dass Schutzvorkehrungen vorgesehen sind. Zudem fehle es insofern weitgehend an einer Gesetzgebungskompetenz des Bundeslandes. Die DVD schließt sich dieser Bewertung an.

Der Gesetzentwurf macht eine Vielzahl weiterer polizeilicher Maßnahmen von einer **drohenden Gefahr** (elektronische Aufenthaltsüberwachung, Art. 15 Abs. 3 Nr. 1,

[16] Dazu kritisch BayLfD (Fn. 4) S. 39 f.; Löffelmann (Fn. 4) Rn. 53-56.
[17] Dazu kritisch BayLfD (Fn. 4), S. 43 ff.; Löffelmann (Fn. 4) Rn. 74.
[18] Dazu kritisch BayLfD (Fn. 4), S. 46 f.; Löffelmann (Fn. 4) Rn. 79 f.
[19] Dazu kritisch BayLfD (Fn. 4), S. 50 ff.; Löffelmann (Fn. 4) Rn. 97.
[20] Dazu kritisch BayLfD (Fn. 4), S. 55 ff., 66
[21] Dazu kritisch BayLfD (Fn. 4), S. 58 ff., 74 ff.; Löffelmann (Fn. 4) Rn. 119; Wächtler, Stellungnahme zu den Gesetzentwürfen der Staatsregierung für ein Gesetz zur Neuordnung des bayerischen Polizeirechts v. 20.03.2018, S. 7 ff.
[22] Dazu kritisch BayLfD (Fn. 4), S. 60 ff.
[23] Dazu kritisch BayLfD (Fn. 4), S. 74.
[24] Stand 26.03.2018, abzurufen unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2018_baypagudna_final.pdf, S. 12.

Bestandsdatenauskunft, Art. 43 Abs. 5 S. 1), evtl. für bedeutende Rechtsgüter (Verarbeitung von besonderen Kategorien personenbezogener Daten, Art. 30 Abs. 2 Nr. 2a, Mustererkennung, Art. 33 Abs. 5 S. 2, Postsicherstellung, Art. 35 Abs. 1 Nr. 1, besondere Mittel der Datenerhebung, Art. 36, polizeiliche Beobachtung, Art. 40 Abs. 1 Nr. 2, Telekommunikationsüberwachung, Art. 42 Abs. 1 Nr. 1, Abs. 4 Nr. 1, Zugriff auf IT-Systeme, Art. 45 Abs. 1 Nr.1, Übermittlung an Geheimdienst, Art. 60 Abs. 3 Nr. 1), abhängig. Dabei wird auf die erst jüngst vorgenommene Einführung dieser Eingriffsschwelle in Art. 11 Abs. 3 S. 2 Nr. 1-5 PAG Bezug genommen, die selbst den Schutz von „erheblichen Eigentumspositionen" einschließt. Mit Eingriffsbefugnissen bei „drohender Gefahr" werden Polizeibefugnisse ins Vorfeld einer Gefahr verlegt, also zu einem Zeitpunkt, in dem noch keine Gefahr besteht, sondern nach Ansicht der Polizei eine Gefahr entstehen könnte. Diese Vorverlagerung von Eingriffsbefugnissen hat das BVerfG bei drohenden terroristischen Straftaten zugelassen, nicht aber etwa bei Bedrohungen „erheblicher Eigentumspositionen".[25] Eine derartige Ausweitung von polizeilichen Standardbefugnissen ist zu unbestimmt und unverhältnismäßig.[26]

Ähnlich problematisch wie die Ausweitung von Befugnisnormen auf (noch) nicht bestehende Gefahren (s. o.) ist die Anknüpfung an Personen und Sachverhalte, die „**mutmaßlich** in Zusammenhang mit der Gefahrenlage stehen" (so z. B. Postsicherstellung beim Nachrichtenmittler, Art. 35 Abs. 1 S. 1 Nr. 2 PAG-E, der Einsatz besonderer Mittel der Datenerhebung gegenüber Kontakt- und Begleitpersonen, Art. 36 Abs. 2 PAG-E, polizeiliche Beobachtung, Art. 40 Abs. 1 Nr. 3 Abs. 2 PAG-E; Telekommunikationsüberwachung Art. 42 Abs. 1 Nr. 2b PAG-E, Eingriff in IT-Systeme, Art. 45 Abs. 1 S. 1 Nr. 2 PAG-E). Dabei greift der Entwurf die grundsätzliche Zulassung polizeilicher Maßnahmen gegenüber Kontakt- und Begleitpersonen auf und entgrenzt die Befugnisse, indem an Stelle einer tatsächlichen Nähe zur Gefahr eine mutmaßliche Nähe genügen soll.[27] Tatsächlich enthält die Rechtsprechung des BVerfG, anders als die Begründung an mehreren Stellen suggeriert (S. 54, 59, 62, 66), keine Rechtfertigung von Eingriffen ausschließlich auf der Grundlage von Mutmaßungen.

Durchsuchung elektronischer Speichermedien

Art. 22 Abs. 2 S. 1 PAG-E erlaubt die Durchsuchung von elektronischen Speichermedien, soweit von einem Durchsuchungsobjekt, also einem körperlichen Gegenstand, „auf sie zugegriffen werden kann". Bei einer derartigen „Durchsuchung" kann es zu Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kommen.[28] Die Regelung enthält keine Vorkehrungen, um Verletzungen des Kernbereichs privater Lebensgestaltung oder den Zugriff auf Daten,

[25] BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09 (Fn. 1), Rn. 112, NJW 2016, 1785.
[26] Kritisch dazu Löffelmann (Fn. 4), Rn. 3-5; Kohnen, 20.03.2017, https://bayrvr.de/2017/03/20/bayerischer-richterverein-stellungnahme-zum-entwurf-eines-gesetzes-zur-effektiveren-ueberwachung-gefaehrlicher-personen/, Nr. 2; Busch, Ein nächster Schritt in Richtung Guantánamo, http://www.grundrechtekomitee.de/node/874, 27.07.2017.
[27] BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09 (Fn. 1) Rn. 116, 168; NJW 2016, 1785, 1791.
[28] BVerfG 27.02.2008 – 1 BvR 370/07 u. 1 BvR 595/07, NJW 2008, 822 = MMR 2008, 315 = DVBl 2008, 582. (Online-Durchsuchung).

die dem Zeugnisverweigerungsrecht nach den §§ 53, 53a StPO unterliegen, zu verhindern. Eine systematische Durchsuchung und **digitale Auswertung** von Festplatten und Cloudinhalten kann nicht mit einer Durchsuchung von körperlichen Sachen gleichgesetzt werden. Die Eingriffsintensität liegt erheblich höher. Dies hat zur Folge, dass zusätzliche Sicherungsmaßnahmen vorgesehen werden müssen, etwa die Regelung eines Richtervorbehalts, die Pflicht zur Protokollierung der Auswertungsmaßnahmen oder die zur Benachrichtigung der Betroffenen.[29]

Bild- und Tonaufnahmen in Wohnungen

Art. 33 Abs. 4 S. 2 PAG-E sieht vor, dass offene Bild- und Tonaufnahmen, etwa durch **polizeiliche Bodycams**, in Wohnungen erstellt und gespeichert werden dürfen „zur Abwehr einer dringenden Gefahr für Leben, Gesundheit oder Freiheit einer Person“, „sofern damit nicht die Überwachung der Wohnung verbunden wird“. Damit erfolgt nicht nur ein Eingriff in das Recht auf informationelle Selbstbestimmung, ins Recht am eigenen Bild und ins Recht am eigenen Wort (Art. 2 Abs. 1 i. V. m. Art. 1 GG) bzw. ins Grundrecht auf Datenschutz (Art. 8 GRCh), sondern auch ein Eingriff in die Unverletzlichkeit der Wohnung (Art. 13 GG, Art. 7 GRCh). Betroffen sind nicht nur Störer, sondern auch mehr oder weniger unbeteiligte Dritte sowie die Polizeibeamten. Die Regelung enthält keine Eingrenzung in Bezug auf besondere Räumlichkeiten, etwa für Psychologen-, Arzt- oder Anwaltspraxen.

Die **Eignung** der Maßnahme für Gefahrenabwehrzwecke ist äußerst umstritten und von einer Vielzahl von Rahmenbedingungen abhängig. Von der Maßnahme können nicht nur disziplinierende, sondern auch aggressionsfördernde Wirkungen ausgehen.[30]

Die geplante Regelung ist eindeutig verfassungswidrig, da sie nicht, wie in Art. 13 Abs. 4 GG vorgesehen, zwingend einen Richtervorbehalt vorsieht. **Art. 13 Abs. 4 GG** regelt nicht nur heimliche, sondern auch offene akustische wie optische Überwachungsmaßnahmen, etwa durch Videokameras, Infrarotkameras oder Mikrophone. Der im Entwurfstext vorgesehene Zusatz „sofern damit nicht die Überwachung der Wohnung verbunden wird“, ändert an dieser klaren Zuordnung nichts, da begriffsnotwendig jeder Kameraeinsatz in einer Wohnung zugleich auch eine Überwachung der Wohnung darstellt. Dass mit der Überwachung vorrangig ein anderes Ziel verfolgt wird, spielt für die Anwendung der objektiv formulierten Anforderungen an Eingriffe in das Wohnungsgrundrecht keine Rolle. Das Wohnungsgrundrecht soll einen Rückzugsraum für die Menschen sicherstellen, der mit jeder Form der optischen oder akustischen Erfassung verletzt wird. Das Grundrecht soll dem Einzelnen gerade in seiner Wohnung zusichern, in Ruhe gelassen zu werden. Dieser Schutz darf nicht durch Abwägung mit Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden.[31]

[29] BayLfD (Fn. 4), S. 10 f.; Löffelmann (Fn. 4), Rn. 14-16; Graulich (Fn. 9), S. 14 ff..
[30] BayLfD (Fn. 4), S. 25; kritisch auch Löffelmann ((Fn. 4) Rn. 32.
[31] BVerfG 03.03.2004 – 1 BvR 2378/98 u. 1 BvR 1084/99, NJW 2004, 999 = DVBl 2004, 557 = MMR 2004, 302 (Großer Lauschangriff), insbes. NJW 2004, 1002.

Ein Rückgriff auf **Art. 13 Abs. 5 GG**, der als Ausnahme vorsieht, dass der Einsatz „ausschließlich zum Schutze der bei einem Einsatz in Wohnungen tätigen Personen“ dient, ist hier nicht möglich, da weder der Gesetzeswortlaut noch die Intention diesen ausschließlichen Schutz als einzigen Zweck im Auge hat.[32] Geschützt werden sollen nicht nur in der Wohnung tätige, sondern auch dritte Personen.

Anders als die Gesetzesbegründung (S. 88) behauptet, kann auch nicht **Art. 13 Abs. 7 GG** als Legitimation herangezogen werden. Danach dürfen Eingriffe „im Übrigen nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, auf Grund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung … vorgenommen werden“. Wegen der abschließenden Regelung in Art. 13 Abs. 4 GG kommt ein Rückgriff auf den subsidiären Art. 13 Abs. 7 GG nicht mehr in Betracht.

Der Verzicht auf einen Richtervorbehalt wird in der Gesetzesbegründung hinsichtlich der weiteren Verwendungen der Aufnahmen „**zu Strafverfahrenszwecken**“ damit gerechtfertigt, dass diese „ohnehin umfassender richterlicher Kontrolle unterliegen“ (S. 89). Dabei wird fälschlich davon ausgegangen, dass ein Strafrichter grds. die Zulässigkeit von Ermittlungsmaßnahmen überprüft; tatsächlich gilt dies nur für die Verwertbarkeit als Beweismittel, wobei andere rechtliche Kriterien gelten.

Optische und akustische Mustererkennung

Gemäß Art. 33 Abs. 5 PAG-E dürfen bei offenen Bild- und Tonaufnahmen im öffentlichen Raum (nicht beim Bodycam-Einsatz) „Systeme zur automatischen Erkennung und Auswertung von Mustern“ zur Erkennung von Sachen und Personen eingesetzt werden, soweit dies erforderlich ist. Insofern stellte sich zunächst die Frage nach der **Geeignetheit** dieser Maßnahme. Bisherige Tests konnten diese mit den heute zum Einsatz kommenden Techniken nicht nachweisen und scheiterten z. B. bei Bildaufnahmen an den Lichtverhältnissen, an der Dynamik der Bilder sowie am Verbergen der identifizierenden Merkmale.[33]

Soweit über die Mustererkennung eine biometrische Identifizierung erfolgen soll, ist Art. 10 DSRl-JI zu beachten, da „**biometrische Daten zur eindeutigen Identifizierung**“ als sensitive Daten bewertet werden (vgl. Art. 3 Nr. 13 DSRl-JI), so dass eine „unbedingte“ Erforderlichkeit bestehen muss und „geeignete Garantien“ vorgesehen werden müssen. Derartige Anforderungen bzw. Garantien enthält der Entwurf aber nicht. Der Verweis auf Art. 39 Abs. 3 S. 1, 2 u. 4 PAG-E, der eine unverzügliche Löschung nach Durchführung des Datenabgleichs ohne Treffer vorsieht, genügt nicht, da zunächst eine verdachtslose Erfassung aller Betroffenen erfolgt. Die spezifischen Risiken der Maßnahme, etwa von Falscherkennungen (false positives), werden nicht adressiert.

[32] Papier in Maunz/Dürig, Grundgesetz, 80. Erg.lfg. Juni 2017, Art. 13 Rn. 107.
[33] Nachweise bei BayLfD (Fn. 4), S. 28.

Die Maßnahme begründet eine schweren Eingriff und hat eine große Streubreite. Insofern wären hohe Anforderungen an Bestimmtheit und an die Eingriffsschwelle zu stellen.[34] Die Regelung ist zu **unbestimmt**, da sie sich nicht auf die Erkennung besonderer Muster (z. B. Gesichtserkennung) beschränkt, sondern über sämtliche biometrische Identifikatoren hinaus jede Form der Mustererkennung erfasst. Dazu gehören z. B. die Erkennung am Gang oder sonstiger Bewegungen. Dazu gehören letztlich auch Detektionen „auffälligen Verhaltens“ von Einzelpersonen wie auch von Menschengruppen per Algorithmus. Da nicht nur Bild-, sondern auch Tonaufnahmen ausgewertet werden können sollen, erfasst die Formulierung sogar die inhaltliche Mustererkennung von Gesprächen. Eine andere Form der Mustererkennung ist die Detektion von bestimmten als gefährlich oder kriminell programmierten Merkmalen von Personen (z. B. Hautfarbe). So wird mit der Regelung eine Rechtsgrundlage geschaffen zur Diskriminierung und Stigmatisierung von Gruppen, die solche Merkmale aufweisen, ohne dass hiergegen angemessene Garantien im Gesetz vorgesehen sind.

Die vorgesehene Mustererkennung stellt eine **automatisierte Entscheidungsfindung im Einzelfall** dar, die in Art. 11 DSRl-JI geregelt ist. Gemäß Art. 11 Abs. 3 DSRl-JI sind Diskriminierungen durch profiling anhand von sensitiven Daten wie biometrischen Identifikatoren oder per Mustererkennung erfassten Daten zum Gesundheitszustand absolut verboten. Gemäß Art. 3 Nr. 4 DSRl-JI ist „Profiling“ „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“.[35] Auch andere Garantien und „zumindest das Recht auf persönliches Eingreifen seitens des Verantwortlichen“, sind nicht, wie in Art. 11 DSRl-JI gefordert, im PAG-E vorgesehen. Weiterhin fehlt es an einer Zweckbeschränkung auf die Gefahrenabwehr und die Strafverfolgung.

Anstatt dass **materiell-rechtlich** hohe Hürden für den Einsatz der Biometrie vorgesehen werden, wird die Mustererkennung als Standardmaßnahme für jede Form der Gefahrenabwehr und darüberhinausgehend sogar als Maßnahme gegen drohende Gefahren zugelassen. Der Verzicht auf eine darüber hinausgehende Beschränkung, etwa auf „im Einzelfall bestehende Gefahren für Leib und Leben“, macht die Regelung unverhältnismäßig und damit unzulässig.[36]

Verdeckter Zugriff auf informationstechnische Systeme

Gemäß Art. 45 Abs. 1 S. 1 Nr. 2 PAG-E wird der verdeckte Zugriff auf **informationstechnische (IT-) Systeme** von Dritten, also nicht nur von (drohenden) Störern erlaubt, soweit Umstände bestehen, dass diese „mutmaßlich“ die Systeme nutzen

[34] Löffelmann (Fn. 4), Rn. 34.
[35] Wortgleich Art. 4 Nr. 4 DSGVO, dazu Buchner in Kühling/Buchner, DSGVO 2. Aufl. 2018, Art. 4 Nr. 4 Rn. 5-8.
[36] Vgl. Hornung/Schindler ZD 2017, 208.

bzw. genutzt haben. Der Zugriff soll verdeckt mit technischen Mitteln erfolgen können. D. h., dass sich die Polizei als Hacker bei Dritten betätigen darf. Hinsichtlich des Hacking-Objektes erfolgt keine weitere Eingrenzung. Erfasst werden sollen nicht nur Geräte, d. h. Hardware von Personen, die zur (drohenden) Gefahr in Zusammenhang gebracht werden, sondern auch Software-Angebote bzw. Applikationen. Damit eröffnet die Regelung den Zugriff auch auf Plattformen wie Facebook oder Google sowie bei Cloud-Datenverarbeitern. Durch die Erlaubnis der Zugriffs auf Zugangsdaten und gespeicherte Daten besteht auch inhaltlich keine Eingriffsbeschränkung (s. o. zu Art. 22 PAG-E). Die Regelung ist zu unbestimmt und zugleich viel zu weit und dadurch unverhältnismäßig.

Einsatz von Drohnen

Art. 47 PAG-E erlaubt den Einsatz unbemannter Flugsysteme für „offene Bild- und Tonaufnahmen“, zur **technischer Erhebung von sonstigen Daten**, etwa aus der Telekommunikation sowie aus IT-Systemen. Mit dieser Befugnis werden Eingriffe in eine Vielzahl von Grundrechten, u. a. auch in das Telekommunikations- und das Wohnungsgrundrecht erleichtert. Spezifische Sicherungs- oder Schutzmaßnahmen sieht die Regelung nicht vor.[37]

Ein Spezifikum von Drohneneinsätzen besteht darin, dass von der Datenerhebung z. B. durch Videoüberwachung nicht nur Störer, sondern typischerweise auch viele völlig **Unbeteiligte betroffen** sind. Eine gezielte Unterscheidung bzgl. der Betroffenen ist zumeist nicht möglich. Damit wird eine verhaltenslenkende und von der Grundrechtswahrnehmung abschreckende Wirkung mit großer Streubreite erreicht, die hohe Schutzvorkehrungen nötig macht, die aber nicht vorgesehen sind.[38]

Der Gesetzestext suggeriert, dass es sich beim Drohneneinsatz nach Absatz 1 Nr. 1 um eine **offene Maßnahme** handeln würde. Relativierend wird in Art. 47 Abs. 2 S. 2 der Hinweis auf die Maßnahme nur als Sollvorschrift formuliert. Tatsächlich ist ein Hinweis oft überhaupt nicht möglich. So können polizeiliche Drohnen von privaten oder sonstigen Drohnen aus der Entfernung weder optisch noch akustisch unterschieden werden. Je größer die Entfernung, umso geringer ist die Wahrscheinlichkeit, dass Drohnen überhaupt als solche erkannt werden. Moderne Sensortechnik ermöglicht es inzwischen, aus großen Entfernungen die gewünschten Datenerhebungen durchzuführen; mit großen Entfernungen kann zugleich der sensorische Erfassungsraum massiv ausgeweitet werden.

Dass es sich beim Drohneneinsatz i. d. R. um einen **verdeckten Einsatz** handelt, ist auch der Regelung selbst zuzuschreiben, die sich nicht auf Bildaufnahmen beschränkt, sondern auch Tonaufnahmen vorsieht sowie elektronische Formen der Datenerfassung. Die Heimlichkeit des Informationsangriffs wird dadurch verstärkt, dass die Betroffenen heute

[37] Kritisch zur Eignung Löffelmann (Fn. 4), Rn. 89.
[38] BVerfG 23.02.2007 – 1 BvR 2368/06, NVwZ 2007, 690 (Videoüberwachung); BVerfG 11.03.2008 – 1 BvR 2074/05 u. 1 BvR 1254/07, NJW 2008, 1505 = MMR 2008, 308 = DVBl 2008, 575 (Kfz-Kennzeichen); BVerfG 11.03.2009 – 2 BvR 941/08, NJW 2009, 3293 = DVBl 2009, 1237 = DÖV 2009, 866 (Geschwindigkeitskontrolle).

grundsätzlich nicht mit einer Datenerfassung aus der Luft rechnen, etwa wenn per Drohne ein Späh- und Lauschangriff durch Fenster auf eine Wohnung erfolgt. Selbst bei Erkennung der Maßnahme ist wegen des flächenabdeckenden Ansatzes insbesondere im öffentlichen Raum, ein Sichentziehen oft überhaupt nicht mehr möglich.[39]

Ist kein Späh- und Lauschangriff auf eine Wohnung geplant und wäre dieser auch materiell-rechtlich nicht zulässig, so gewährleistet die Regelung nicht, dass ein solcher Angriff auch nicht erfolgt, indem bei der Datenerhebung über Fenster in **Wohnungen** eingedrungen wird oder dass von oben vom Boden nicht einsehbare, zur Wohnung gehörende Bereiche erfasst werden.

Die Kombination des Drohneneinsatzes mit anderen Datenerhebungs- und Auswertungsbefugnissen, etwa der Mustererkennung, eröffnet Überwachungspotenziale von orwellschem Ausmaß und totalitärer Qualität. Die Regelung ist somit zu unbestimmt und greift in unverhältnismäßiger Form und ohne die nötigen Schutzvorkehrungen in eine Vielzahl von Grundrechten ein und ist **verfassungswidrig**.

Überwachungsgesamtrechnung

Der Gesetzentwurf enthält in seiner Gesamtheit von informationellen Eingriffsbefugnissen Erlaubnisse zur Überwachung der Bevölkerung, die über das vom BVerfG erlaubte Maß hinausgehen. Das BVerfG hat dargelegt, dass eine Gesetzgebung, „die auf eine möglichst **flächendeckende vorsorgliche Speicherung** aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte, … von vornherein mit der Verfassung unvereinbar“ ist.[40] Es muss sichergestellt werden, dass nicht alle Aktivitäten der Bürgerinnen erfasst und rekonstruiert werden können. „Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem ´additiven` Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt“.[41] Diesen grundsätzlichen verfassungsrechtlichen Anforderungen genügt der Entwurf nicht. Er enthält Ermittlungsbefugnisse weit im Vorfeld von Gefahren sowie gegenüber jedermann und schöpft dabei die technischen Möglichkeiten der Überwachung weitestgehend aus, ja sieht teilweise sogar Überwachungsmaßnahmen vor, die technisch heute noch nicht machbar sind, ohne adäquate Grundrechtssicherungen vorzusehen.[42]

Ergebnis

Der Entwurf für eine Neuordnung des bayerischen Polizeiaufgabengesetzes ist **in seinem gesamten Regelungsinhalt verfassungswidrig**. Die mit ihm vertiefte Abkehr von den Anforderungen an eine konkrete Gefahr als Anlass und einen Störer als Adressat der Maßnahmen eröffnet es der Polizei ohne adäquate Einschränkungen personenbezogene

[39] Weichert ZD 2012, 503.
[40] BVerfG 02.03.2010 – 1 BvR 256/08 u. a., BVerfGE 125, 323 (Vorratsdatenspeicherung).
[41] BVerfG 20.04.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, Rn. 130, BVerfGE 141 280 f.
[42] BayLfD (Fn. 4), S. 2 f.; Löffelmann (Fn. 4), Rn. 6, 121 f.; Wächtler (Fn. 21), S. 1 ff.

Daten zu erheben und damit in Grund- und Freiheitsrechte einzugreifen. Dabei wird oft weder die Eignung, geschweige die (unbedingte) Erforderlichkeit für die Gefahrenabwehr dargelegt und zur Voraussetzung gemacht. Selbst noch nicht bestehenden technischen Möglichkeiten wird für die Zukunft die Tür geöffnet, ohne dass Erfahrungen mit diesen gesammelt und deren Risiken bewertet werden konnten. Letztlich signalisiert der Entwurf an die Polizei: Alles ist möglich. Dies hat zur Folge, dass die Menschen begründet befürchten müssen, dass auch Alles gemacht wird und dass weder Transparenz- noch Kontrollmechanismen eine Eingrenzung sicherstellen. Dadurch ausgelöste Verunsicherung beeinträchtigt die Menschen nicht nur in der Wahrnehmung ihrer Freiheitsrechte, sondern auch deren Vertrauen in die Polizei. Mit der Entgrenzung der polizeilichen Befugnisse wird der PAG-E zum Bärendienst für die Polizei.

Durch die Pflicht, mit dem Polizeirecht die DSRl-JI, also europäisches Recht, umzusetzen, ist das PAG nicht nur am nationalen Verfassungsrecht, sondern auch am **europäischen Recht** und insbesondere an der europäischen Grundrechte-Charta (GRCh) zu messen. Die dadurch vorgegebenen Anforderungen entsprechen weitgehend denen des nationalen Verfassungsrechts, gehen aber teilweise, etwa bei den Diskriminierungsverboten (Art. 21 GRCh) darüber hinaus. Die Anwendbarkeit des Europarechts hat zur Folge, dass Gerichte – sollten sie insofern einen Verstoß erkennen – ein Vorlageverfahren beim Europäischen Gerichtshof initiieren können (Art. 267 AEUV).

Bevor der Bayerische Landtag eine Ausweitung der Befugnisse im Polizeirecht vorsieht, ist er aufgefordert, bezüglich der bestehenden Regelungen Europarechts- und Verfassungskonformität herzustellen. In einem weiteren Schritt könnte über eine Evaluation festgestellt werden, inwieweit durch den Wandel der Gefahren und der technischen Möglichkeiten Ergänzungsbedarfe bestehen. Es steht zur befürchten, dass der Landtag diesem Rat nicht folgen wird. Umso wichtiger ist es, frühzeitig und umfassend die neuen Befugnisse öffentlich zu erörtern. Im aktuellen Gesetzgebungsverfahren bestehen hierfür nicht (mehr) die nötige Zeit und der nötige Rahmen. Problematische Regelungen sollten **so früh wie möglich auf den rechtlichen Prüfstand** gestellt werden. Nur so kann verhindert werden, dass die bayerischen Regelungen zum Vorbild für andere Bundesländer oder gar für den nationalen Gesetzgeber genommen werden.