

Stellungnahme des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

zu den Verfassungsbeschwerdeverfahren gegen die Neuregelung der Vorratsdatenspeicherung unter den Aktenzeichen

1 BvR 141/16

1 BvR 229/16

1 BvR 2023/16

1 BvR 2683/16

~~1 BvR 2821/16~~

I. Vorbemerkungen

Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (BGBl. 2015 I Nr. 51, S. 2218) vom 10. Dezember 2015 beinhaltet unter anderem Änderungen der Strafprozessordnung (StPO) in Bezug auf die Erhebung und Verarbeitung von Verkehrsdaten (§§ 100g, 101a, 101b StPO) sowie Änderungen des Telekommunikationsgesetzes (TKG) hinsichtlich der Speicherung und Verwendung der Verkehrsdaten (§§ 113b, 113c TKG). Diese Änderungen haben die anlasslose Speicherung von Telekommunikationsdaten – Verkehrsdaten – durch die Telekommunikationsunternehmen als Verpflichtete zur Folge sowie die Übermittlung dieser anlasslos erhobenen Daten an die Sicherheitsbehörden nach Maßgabe des TKGs und der korrespondierenden Gesetze der jeweiligen Strafverfolgungs- oder Gefahrenabwehrbehörde.

Der Umfang, die Vielschichtigkeit und Detailtiefe der gegenständlichen Verfassungsbeschwerden verdeutlichen einmal mehr die rechtliche wie technische Komplexität der Thematik Vorratsdatenspeicherung. Der Bayerische Landesbeauftragte für den Datenschutz greift in seiner Stellungnahme insbesondere die technischen Entwicklungen in Bezug auf die Internetnutzung auf, die seit 2010 auf die Telekommunikation einwirken. Die aktuellen technischen Gegebenheiten werden nicht angemessen durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten abgebildet. Dies hat Auswirkungen auf die Beurteilung der Verfassungsmäßigkeit des Gesetzes. Kritik wird insbesondere an der mangelnden Normenklarheit der einschlägigen Regelungen des Telekommunikationsgesetzes geübt. Außerdem wird das Gesetz unter anderem dahingehend bemängelt, dass es die verfassungsrechtlichen Anforderungen an eine Vorratsdatenspeicherung, die von dem Bundesverfassungsgericht in seinem Urteil vom 2. März 2010¹ aufgestellt wurden, nicht ausreichend berücksichtigt. Diesen Ausführungen schließe ich mich ausdrücklich an.

Die vorliegende Stellungnahme wird sich unter Berücksichtigung der eingehenden Ausführungen zu den zahlreichen verfassungs- und europarechtlich möglicherweise relevanten Aspekten der Neuregelung der Vorratsdatenspeicherung in der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofes auf den Aspekt des additiven Grundrechtseingriffs in der Ausprägung konzentrieren, die er in der vorgenannten Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung aus dem Jahr 2010 gefunden hat.²

¹ Vgl. BVerfGE 125, 260.

² Vgl. BVerfGE 125, 260 (323 f.).



Ausgangspunkt ist die Frage, ob die im deutschen Sicherheitsrecht nun insgesamt verankerten Möglichkeiten der Erhebung und Verarbeitung personenbezogener Daten zu Zwecken der Strafverfolgung und Gefahrenabwehr zu einem in der Gesamtschau noch verfassungsmäßigen Bestand an die Überwachung des Einzelnen ermöglichenden informationellen Eingriffsbefugnissen und entsprechenden Dateien führen oder ob diese Grenze überschritten sein könnte. Im Zentrum der Erwägungen stehen Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), aber auch das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 GG), das Recht auf die Vertraulichkeit und Integrität informationstechnischer Systeme oder das Telekommunikationsgeheimnis (Art. 10 GG) kommen als verletzte Grundrechte in Betracht. Besondere Berücksichtigung bei dieser Wertung soll insoweit die Umsetzung der Richtlinie (EU) 2016/681 durch das Fluggastdatengesetz (FlugDaG) finden. Darüber hinaus werden einige im vorgenannten Zusammenhang möglicherweise bedeutsame Aspekte des Datenaustauschs zwischen den Sicherheitsbehörden im föderalen System aufgegriffen.

II. Additiver Grundrechtseingriff und Vorratsdatenspeicherung

In seiner ersten Entscheidung zur Verfassungsmäßigkeit der Vorratsdatenspeicherung hat das Bundesverfassungsgericht zu den Grenzen der Vorratsspeicherung von für die Gefahrenabwehr und Strafverfolgung verwertbaren Daten insbesondere ausgeführt:

„(D)ie Speicherung der Telekommunikationsverkehrsdaten (darf) nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielt. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt vielmehr voraus, dass diese eine Ausnahme bleibt. Sie darf auch nicht im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen. (...) Die Einführung der Telekommunikationsverkehrsdatenspeicherung kann damit nicht als Vorbild für die Schaffung weiterer vorsorglich anlassloser Datensammlungen dienen, sondern zwingt den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der vorhandenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (...).“³

Auf Grundlage dieser Passage wird teilweise in Verwandtschaft zum Begriff des additiven Grundrechtseingriffs von einer „Überwachungs-Gesamtrechnung“ gesprochen⁴, auf die auch im aktuellen Diskurs über die Reform landesgesetzlicher Regelungen im Gefahrenabwehrrecht und Strafprozessrecht zur Erhebung und Verarbeitung personenbezogener Daten gelegentlich Bezug genommen wird.⁵

Während sich die genannten Ausführungen zur Vorratsdatenspeicherung noch auf die äußerste Grenze der Kumulation von Datensammlungen beziehen, die die Erfassung von Daten insgesamt

³ BVerfGE 125, 260 (323 f.).

⁴ Seit *Roßnagel* NJW 2010, 1238 (1240 f.).

⁵ Vgl. insbesondere *Petri*, Stellungnahme zur Reform des Bayerischen Polizeiaufgabengesetzes vom 21.12.2017, S. 2 f., abgerufen unter: <https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf> (zuletzt geprüft am 26.3.2018); *Arzt* DÖV 2017, 1023 (1027); *Knierim* ZD 2011, 17 (20 f.); *Roßnagel* NJW 2010, 1238 (1240 f.).

dergestalt beschränkt, dass nicht praktisch alle Aktivitäten der Bürger durch Sicherheitsbehörden rekonstruierbar sein dürfen⁶, wird in der Entscheidung des angerufenen Gerichts zur Verfassungsmäßigkeit des Bundeskriminalamtgesetzes ein ähnlicher Gedanke mit Blick auf die Kumulation verschiedener Informationseingriffe durch die Sicherheitsbehörden gegen eine Person entwickelt. Eigene verfassungsrechtliche Grenzen ergäben sich hinsichtlich des Zusammenwirkens der unterschiedlichen Überwachungsmaßnahmen. Es sei mit der Menschenwürde unvereinbar, wenn eine Überwachung sich über einen längeren Zeitraum erstrecke und derart umfassend sei, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert würden und zur Grundlage für ein Persönlichkeitsprofil werden könnten. Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssten die Sicherheitsbehörden mit Rücksicht auf das dem ‚additiven‘ Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibe.⁷

Diese Grundsätze bezogen sich zwar unmittelbar nur auf die Grenzen der Verhältnismäßigkeit bei der kumulierten Anwendung gesetzlich möglicher Einzelmaßnahmen durch Sicherheitsbehörden⁸, sollten aber vor dem Hintergrund der vorstehenden Erwägungen zu den Wirkungen weitreichender und vielfältiger sicherheitsbehördlicher Dateien auch auf gesetzgeberischer Ebene Berücksichtigung finden.

Die Kombination unterschiedlicher Dateien, die für sich genommen der genannten Gesamtgrenze noch genügen mag, sollte in der Betrachtung mit dem Umfang der Zugriffsmöglichkeiten und der Kombination mit vielfältigen ebenfalls technisch gestützten Maßnahmen durch eine Vielzahl von Sicherheitsbehörden in dem föderalen Mehrebenensystem einschließlich folgender Übermittlungsmöglichkeiten in einer Gesamtschau betrachtet und bewertet werden.

Die genannten Regelungen zu Informationseingriffen mögen zwar nicht den in der ersten Vorratsdatenspeicherung angesprochenen Verfassungskern einer totalen Erfassung und Registrierung der bürgerlichen Freiheitswahrnehmung⁹ berühren, können aber in ihrer Gesamtheit gerade infolge des Austauschs zwischen unterschiedlichen Sicherheitsbehörden im föderalen System potentiell zu einer an die Grenze der Totalität reichenden *Erfassbarkeit* der personenbezogenen Daten jeder Bürgerin und jedes Bürgers führen. Dies gilt mit Blick auf die seit 2010 nochmals erheblich fortgeschrittene Digitalisierung auch gerade für den weiter massiv anwachsenden Bestand telekommunikativ oder durch Nutzung informationstechnischer Systeme erzeugter personenbezogener Daten jeder und jedes Einzelnen.¹⁰

Bereits dieses Potential der individuellen Totalerfassung kann aber die vom Bundesverfassungsgericht verschiedentlich angesprochene Gefahr eines „diffus bedrohliche(n) Gefühl(s) des Beobachtetseins“ auslösen¹¹, dass den im demokratischen Interesse liegenden individuellen Freiheitsgebrauch zu beeinträchtigen geeignet ist¹², indem es die gesellschaftlichen Grundlagen eines

⁶ BVerfGE 125, 260 (323 f.).

⁷ BVerfGE 141, 220 (280 f.).

⁸ Petri, Stellungnahme zur Reform des Bayerischen Polizeiaufgabengesetzes vom 21.12.2017, S. 2, abgerufen unter: <https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf> (zuletzt geprüft am 26.3.2018).

⁹ BVerfGE 125, 260 (323 f.).

¹⁰ Vgl. auch Petri, Stellungnahme zur Reform des Bayerischen Polizeiaufgabengesetzes vom 21.12.2017, S. 1, abgerufen unter: <https://www.datenschutz-bayern.de/1/PAG-Stellungnahme.pdf> (zuletzt geprüft am 26.3.2018).

¹¹ Vgl. BVerfGE 125, 260 (320).

¹² Vgl. BVerfGE 65, 1 (43).



unbefangenen demokratischen Diskurses, den „freiheitlichen Kerngehalt der Gesellschaftsordnung“¹³ unterminiert.

III. Potentiell unzulässige Totalüberwachung infolge der anlasslosen Neuerhebung durch das Fluggastdatengesetz und Übermittlungsregelungen

Im Unterschied zum Jahr 2010 ist das bestehende Potential individueller Totalerfassbarkeit gewachsen. Beispielhaft wird auf die Kombination der Telekommunikationsverkehrsdatenspeicherung mit der anlasslosen Speicherung von Fluggastdaten und einige in Betracht zu ziehende Übermittlungsvorschriften und Verbunddateien eingegangen.

1. Anlasslose Erhebung und Verarbeitung personenbezogener Daten durch das Fluggastdatengesetz (FlugDaG)

Das am 6. Juni 2017 ausgefertigte Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz, FlugDaG) ordnet die Übermittlung umfangreicher Datensätze aller Fluggäste von Flügen an, die von deutschen Flughäfen ausgehen, dort enden oder zwischenlanden. Die Übermittlung wird durch die Luftfahrtunternehmen an das Bundeskriminalamt vorgenommen (§ 2 f. FlugDaG). Die Speicherung erfolgt für 5 Jahre (§ 13 FlugDaG), nach 6 Monaten soll eine sog. Depersonalisierung erfolgen, die jedoch umkehrbar ist (§ 5 FlugDaG). Dies führt zu Speichervolumen innerhalb des Fünfjahreszeitraums von rund 850 Millionen Fluggastdatensätzen.¹⁴

Nach § 4 FlugDaG gleicht das Bundeskriminalamt die erhobenen Daten mit „Datenbeständen“ und „Mustern“ ab. Ziel ist es ausweislich der Vorschrift, „Personen zu identifizieren, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie (...) Straftaten“ (eines dann folgenden Straftatenkataloges) „begangen haben oder innerhalb eines übersehbaren Zeitraums begehen werden“. Es handelt sich insoweit also um eine auf einen bestimmten Lebensbereich bezogene, aber dennoch von erheblicher Streubreite gekennzeichnete Kombination anlassloser Informationseingriffe¹⁵, die teilweise denen der Kfz-Kennzeichenüberwachung und teilweise der präventiven Rasterfahndung ähneln. Die in § 4 FlugDaG benannten Abgleiche mit Datenbeständen und Mustern stellen daher anlasslose „Verdachts-“ oder „Verdächtigengewinnungseingriffe“ dar.¹⁶

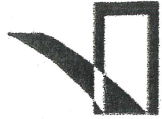
Die durch diese Abgleiche erhobenen Fluggastdatensätze und zusätzliche Informationen können nach § 6 Abs. 1 FlugDaG zur weiteren Verarbeitung und Veranlassung weiterer Maßnahmen an andere Abteilungen des Bundeskriminalamts, an die Landeskriminalämter, die Zollverwaltung und die Bundespolizei übermittelt werden. Soweit diese Behörden Aufgaben der Strafverfolgung wahrnehmen, können sie die übermittelten Daten zu anderen Zwecken verarbeiten, wenn Erkenntnisse, auch unter Einbezug weiterer Informationen, den Verdacht einer bestimmten anderen Straftat begründen (§ 6 Abs. 4 FlugDaG). Darüber hinaus können die genannten Daten auch an die Nachrichtendienste des Bundes und der Länder zur Erfüllung von deren Aufgaben übermittelt werden (§ 6 Abs. 2 FlugDaG). Dann besteht aber, wie auch bei den in Abs. 1 genannten Behörden, soweit diese keine Aufgaben der Strafverfolgung wahrnehmen, eine Begrenzung auf den Übermittlungszweck (§ 6 Abs. 3 FlugDaG).

¹³ Knierim ZD 2011, 17 (19).

¹⁴ Arzt DÖV 2017, 1023 (1024) mwN.

¹⁵ Vgl. dazu BVerfGE 141, 220 (268).

¹⁶ Vgl. Arzt DÖV 2017, 1023 (1025).



Die §§ 7-10 FlugDaG (ab dem 25. Mai 2018 in Kraft) ordnen in Vollzug des europäischen Ansatzes zur Verkehrsfähigkeit personenbezogener Daten und der Zusammenarbeit im Bereich der Kriminalitätsbekämpfung und der Gefahrenabwehr weitreichende Übermittlungsmöglichkeiten an andere Mitgliedstaaten und auch Drittstaaten an. Insbesondere kann nach § 9 FlugDaG auch Europol auf die Daten zugreifen.

Perspektivisch ist auf europäischer Ebene darüber hinaus angedacht, dezentrale Systeme, die auf der Grundlage der Richtlinie über Fluggastdatensätze betrieben werden, zu einem späteren Zeitpunkt mit einer oder mehreren der im Rahmen der Verordnung zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen¹⁷ vorgeschlagenen Komponenten verknüpft werden, sofern nachgewiesen wird, dass dies notwendig ist.

Die Kumulation von Telekommunikations-Vorratsdatenspeicherung und Fluggastdatenspeicherung führt nach hier vertretener Auffassung zu einem verfassungsrechtlich nicht mehr akzeptablen Übermaß an staatlicher Überwachung.¹⁸

Die heimliche und anlasslose Abgleichung der Fluggastdaten mit kriminalistisch entwickelten Mustern kann eine bestimmte verdachtsbegründende Tatsachengrundlage im Sinne des § 100g StPO darstellen und – wegen § 6 Abs. 4 FlugDaG – unabhängig vom Straftatenkatalog des § 4 Abs. 1 FlugDaG eine sich allein nach § 100g StPO richtende Erhebung von Verkehrsdaten rechtfertigen.

Weil die betroffenen Personen auf die Gestaltung der beim Bundeskriminalamt entwickelten Muster keinen Einfluss haben und diese auch nicht allgemein bekannt sind, kann es dergestalt, ohne dass die betroffenen Personen hierfür in zurechenbarer Weise einen Anlass gesetzt haben, und ohne dass sie davon vorher erfahren, zu einer Kombination der nach § 113b TKG und § 2 FlugDaG gespeicherten Datensätze kommen.

Das bedeutet konkret, dass bei der strafverfolgenden Behörde dann u.a. alle möglichen Informationen den Flug betreffend, Zahlungsinformationen einschließlich der Rechnungsanschrift (§ 2 Abs. 2 Nr. 10 FlugDaG), durch bei Flugbuchung vorzulegende Identitätsdokumente verifizierte Informationen über Staatsangehörigkeit, Familiennamen, Vornamen, Geschlecht, Geburtsdatum einschließlich Art, Nummer, Ausstellungsland und Ablaufdatum von Identitätsdokumenten (§ 2 Abs. 2 Nr. 8 FlugDaG), aber auch Daten über die ungefähren Aufenthaltsorte der letzten vier Wochen (§ 113b Abs. 1, 4 TKG) und über sämtliche Telekommunikationsverbindungen (E-Mail, Telefon, Mobiltelefon etc., § 113b Abs. 2, 3 TKG) vorliegen.

Vor dem Hintergrund der steigenden Nutzungsintensität von Telekommunikationsdiensten und Diensten der Informationsgesellschaft im Zuge der Digitalisierung führt dies dazu, dass die Verarbeitung der Fluggastdaten zu einem Einfallstor für die nahezu lückenlose Dokumentation zumindest des vergangenen Monats im Leben von betroffenen Personen darstellen kann, ohne dass diese hierfür selbst erkennbar einen Anlass gesetzt haben oder hiervon erfahren.

2. Weiterverarbeitung und Übermittlung

Die Speicherung der in § 2 Abs. 1 FlugDaG genannten Fluggastdaten dient dazu, allein aufgrund kriminalistischer Muster zu einem Anfangsverdacht oder gegebenenfalls der Annahme einer kon-

¹⁷ Vorschlag einer Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (Grenzen und Visa) und zur Änderung der Entscheidung 2004/512/EG des Rates, der Verordnung (EG) Nr. 767/2008, des Beschlusses 2008/633/JI des Rates, der Verordnung (EU) 2016/399 und der Verordnung (EU) 2017/2226 (COM(2017) 793 final) in der Fassung vom 12. Dezember 2017.

¹⁸ Ebenso schon Arzt DÖV 2017, 1023 (1027); ausdrücklich unter Bezug auf Flugverkehrsdaten Roßnagel NJW 2010, 1238 (1240); Knierim ZD 2011, 17 (23).

kreten Gefahr zu kommen und ermöglicht schon ausweislich des § 6 FlugDaG die Übermittlung an unterschiedliche Sicherheitsbehörden. Diese Behörden, aber auch das Bundeskriminalamt selbst, haben die den Anfangsverdacht oder die Gefahrenannahme begründenden Tatsachen dann regelmäßig in sicherheitsrechtliche Informationssysteme wie INPOL (§ 11 BKAG) oder die Antiterrordatei (§ 2 ATDG: „tatsächliche Anhaltspunkte“) einzustellen.

Des Weiteren können aufgrund eines nach Maßgabe des Musterabgleichs¹⁹ gewonnenen Verdachts in diesen Dateien regelmäßig auch Abfragen vorgenommen werden. Diese ermöglichen im Fall der Antiterrordatei zunächst Anbahnungstreffer²⁰, in der Folge aber zumindest teilweise nach den Übermittlungsvorschriften auch den Zugriff auf anderweitig vorgehaltene Daten. Dies dürfte z.B. hinsichtlich der dem Bundesnachrichtendienst aufgrund der strategischen Telekommunikationsüberwachung vorliegenden Inhaltsdaten nach § 7 Abs. 4 G10 („tatsächliche Anhaltspunkte für [einen] Verdacht“ oder bestimmte „bestimmte [verdachtsbegründende] Tatsachen“) regelmäßig der Fall sein.

Darüber hinaus stellt der durch den Abgleich nach § 4 FlugDaG generierte (repressive oder präventive) Verdacht aber auch die Tatsachengrundlage für zahlreiche weitere (Informations-)Eingriffe aufgrund eigenständiger Ermächtigungsgrundlagen der mit Polizeiaufgaben betrauten Behörden dar. In zahlreichen Gesetzen bestehen heute Ermächtigungsgrundlagen für Informationseingriffe, deren Eingriffschwelle aufgrund des gewonnenen Verdachts oder der Tatsachengrundlage für eine konkrete Gefahr erreicht sein kann. Eine Reihe dieser Ermächtigungsgrundlagen bestanden in dieser Form im Jahr 2010 noch nicht. Derartige Vorschriften finden sich unter anderem im Bundeskriminalamtsgesetz. In einigen Ländern sind Gesetzesänderungen erfolgt (z.B. Bayern) oder vorgesehen (z.B. Nordrhein-Westfalen), die den jeweiligen Polizeibehörden weitreichende neue informationelle Eingriffsbefugnisse und mehr Vorfeldbefugnisse verschaffen.

Die Inhalte solcher Regelungen sind weit reichend. So soll sich in Zukunft die sog. „Quellen-Telekommunikationsüberwachung“ in zahlreichen landes- und bundesrechtlichen Regelwerken finden, die Möglichkeiten der Videoüberwachung, teilweise einschließlich der Erkennung biometrischer Merkmale soll ausgeweitet werden und weitere Vorverlagerungen sollen durch die Einführung der Gefahrenkategorie der sog. „drohenden Gefahr“ erfolgen.²¹

IV. Abschließende Stellungnahme

Die Vorschriften über die Vorratsdatenspeicherung, des Gesetzes über die Verarbeitung von Fluggastdaten, die Vorschriften über INPOL, die Antiterrordatei, die strategische Telekommunikationsüberwachung durch den Bundesnachrichtendienst und zahlreiche bereits erlassene und teilweise geplante erweiterte gesetzliche Ermächtigungen zur Datenverarbeitung zu Zwecken der Gefahrenabwehr und Strafverfolgung in Bund und Ländern haben auch dann, wenn sie jeweils für sich genommen den Vorgaben des Grundgesetzes noch genügen sollten, in ihrer Kombination das Potential massiver additiver Grundrechtseingriffe im Einzelfall bis hin zur Grenze der Totalüberwachung. Das Gesetz über Fluggastdaten ist als Umsetzung von Unionsrecht zumindest in die Be-

¹⁹ Arzt DÖV 2017, 1023 (1023, 1025) – „Kleine Rasterfahndung“.

²⁰ Vgl. zur eingriffsmildernden Wirkung dieses Umstands BVerfGE 133, 277 (329 ff.).

²¹ Vgl. zum nordrhein-westfälischen Gesetzentwurf der Landesregierung zur Stärkung der Sicherheit <https://www.landtag.nrw.de/Dokumentenservice/portal/WWW/dokumentenarchiv/Dokument/MMV17-569.pdf?jsessionid=7E62D22B0D73F7B8B0F357D054A8DCBA.ifxworker> und zum besonders weitreichenden bayerischen Pendant <https://www.datenschutz-bayern.de/1/PAG-neu.pdf> (zuletzt abgerufen am 27.3.2018).

wertung einzubeziehen, verfassungsrechtliche Konsequenzen betreffen vorliegend zuvörderst das Telekommunikationsgesetz.

Eingriffe können die Erhebung und Verarbeitung personenbezogener Daten einer Einzelperson in erheblichem Umfang über einen erheblichen Zeitraum umfassen und sie ermöglichen weitreichende Rückschlüsse auf etwa das Sozialverhalten, den Aufenthalt oder auf Kontaktpersonen. Sie können erfolgen, ohne dass die betroffene Person hierfür einen erkennbaren Anlass gesetzt hat, ferner ohne dass sie dies erfährt und zu den verdachtsbegründenden Tatsachen Stellung nehmen kann. Diese Eingriffe betreffen vorrangig das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), sie berühren aber weitere Grundrechte der Kommunikation und verkürzen die informatorische Rechtstellung des Bürgers insgesamt.

Zudem können Betroffene in erheblichem Umfang spürbaren Folgemaßnahmen aufgrund der Gefahrenabwehrgesetze und der Strafprozessordnung ausgesetzt sein, denn zahlreiche, auch nicht-informatorische, Eingriffe setzen nicht mehr als einen Anfangsverdacht oder eine konkrete Gefahr voraus. Diese Eingriffsschwelle kann aufgrund der anlasslosen Erhebung von Daten und deren Verarbeitung insbesondere durch die heimliche Verknüpfung mit anderweitig heimlich erhobenen Daten sehr schnell überwunden werden.

Damit ist die totale und heimliche Erfassbarkeit praktisch aller den täglichen Freiheitsgebrauch betreffenden personenbezogenen Daten durch die Sicherheitsbehörden grundsätzlich in den Bereich des Möglichen gerückt. Die von einem solchen Überwachungspotential ausgehenden Einschüchterungswirkungen und ihre erheblichen Gefahren für die gesellschaftlichen Voraussetzungen der unbefangenen durch Grundrechte geschützten Kommunikation gebieten, dass sich der Gesetzgeber bei der Auswahl anlasslos zu sammelnder Datenbestände beschränkt und gegebenenfalls für nur einige der möglichen Maßnahmen entscheidet oder erhebliche Einschränkungen bei der Übermittelbarkeit und Vernetzbarkeit personenbezogener Daten unter den Sicherheitsbehörden vornimmt. Wegen der immer weiter reichenden Kooperationsformen und Übermittlungsmöglichkeiten zwischen Bund und Ländern darf sich der Blick hierbei auch nicht auf jeweils nur einen Rechtsträger beschränken.

Verfahrensmäßige Absicherungen zur Verhinderung einer potentiell möglichen heimlichen Totalüberwachung sind zwingend erforderlich, reichen allerdings für sich genommen nicht aus, um den für die freiheitliche Demokratie konstitutiven Schutz der Grundrechte zur Freiheitsausübung im Kommunikationsraum und das erforderliche Vertrauen der Bürgerinnen und Bürger in die Wahrung ihrer Privatheit zu gewährleisten.²² Der Gesetzgeber muss auch inhaltliche Kriterien zur Eingrenzung der Befugnisse anlegen wie etwa die Anlassbezogenheit oder Offenheit der Datenerhebung und Datenverarbeitung, die sich aus der Rechtsprechung ableiten lassen.²³

Im Ergebnis ist aufgrund der weit reichenden Möglichkeiten additiv zu betrachtender Informations-eingriffe an einschlägige gesetzliche Regelungen in jedem Fall ein strikter Maßstab der Verhältnismäßigkeit anzulegen.²⁴ Darüber hinaus sind anlasslose Eingriffe mit erheblicher Streubreite wie die Vorratsdatenspeicherung grundsätzlich unzulässig, weil sie aufgrund der Rechtslage in Kumulation mit weiteren Eingriffen die Schwelle zur Option der Totalüberwachung überschreiten.

²² Vgl. zu den Risiken einer fortschreitenden Überwachung aufgrund fortschreitender Technisierung in anderem Kontext schon das Minderheitsvotum in BVerfGE 109, 279 (390 f.).

²³ Überblick bei Kugelman, Staatliche Überwachung und Grundrechte, insbesondere rechtliche Grenzen des Einsatzes von Bodycams, in: Dominique Hascher, Peter Jung, Timothée Paris und Götz Schulze (Hrsg.), Sicherheit und Freiheit - 12. Deutsch-französisches Juristentreffen an der Universität Potsdam, Tübingen 2018, S. 127 ff.

²⁴ Vgl. BVerfGE 141, 220 (280 f.).