GESELLSCHAFT FÜR FREIHEITSRECHTE

20. Juni 2024

Stellungnahme

zum Gesetzentwurf der Bundesregierung „Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes“ (BT-Drs. 20/10859)

für die öffentliche Anhörung im Ausschuss für Inneres und Heimat des Deutschen Bundestags am 24. Juni 2024

von Dr. Simone Ruf,
Gesellschaft für Freiheitsrechte e.V.

A. Zusammenfassung

Hinsichtlich der im Gesetzentwurf der Bundesregierung vorgesehenen Reformen des Bundesdatenschutzgesetzes (im Folgenden „BDSG“) empfehlen wir, insbesondere die Erweiterung der Ausnahmen zu den datenschutzrechtlichen Auskunftsansprüchen in § 34 Abs. 1 Satz 2 BDSG-E und § 83 Abs. 1 Satz 2 SGB X-E zu streichen. Dies würde Betroffenenrechte und den Rechtsschutz gegen rechtswidrige Datenverarbeitungen erheblich schwächen (B).

Zwar begrüßen wir die Aufnahme von § 16a BDSG-E. Die Institutionalisierung der Datenschutzkonferenz (im Folgenden „DSK“) könnte aber grundsätzlich noch weiter gehen und auch eine Geschäftsstelle sowie eine verbindliche Beschlussfassung vorsehen (C).

Da der Einsatz biometrischer Fernidentifikationssysteme auch in Deutschland in der polizeilichen Praxis trotz fehlender Rechtsgrundlagen auf dem Vormarsch ist, empfehlen wir, die Gelegenheit der Reform des BDSG zu nutzen, den Gesetzentwurf durch ein **Verbot** von Datenverarbeitungen mittels **biometrischer Fernidentifikationssysteme im öffentlichen Raum** zu erweitern (D).

Der Einsatz derartiger Systeme ist mit enormen Risiken und Gefahren für Grund- und Menschenrechte verbunden und kann angesichts der nach wie vor hohen Fehleranfälligkeit und Diskriminierungseffekte dieser Systeme nicht zu einer effektiven Polizeiarbeit beitragen. Angesichts des Missbrauchspotenzials muss ein Einsatz durch Private erst recht ausgeschlossen sein.

Das Unionsrecht lässt den nationalen Gesetzgebern Spielraum für ein solches Verbot und auch das Grundgesetz ermöglicht es, Verbote im Rahmen der verfassungsrechtlichen

Kompetenzordnung im BDSG vorzusehen. Die Verbote können für öffentliche Stellen der Länder zwar nur eingeschränkt Geltung beanspruchen, jedoch erweitert § 500 StPO den Anwendungsbereich des BDSG für die Tätigkeit der Landespolizei im repressiven Bereich.

Wir empfehlen ein möglichst umfassendes Verbot, welches Echtzeit- als auch retrograde Abgleiche umfasst. Diese pauschale, auf der KI-Verordnung basierende Unterscheidung ist aus grundrechtlicher Perspektive nur schwer nachvollziehbar und jedenfalls nicht das ausschlaggebende Kriterium für die Beurteilung der Eingriffsintensität. Vielmehr birgt auch der retrograde Abgleich das Risiko nachhaltiger Grundrechtsbeeinträchtigungen und spezifischer Gefahren.

Wir empfehlen, auch die Weiterverarbeitung von Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme in öffentlich zugänglichen Räumen aufgrund anderer Gesetze erhoben wurden, zu verbieten. Dadurch können potenzielle Lücken geschlossen werden, die sich gegebenenfalls künftig daraus ergeben könnten, dass auf Landesebene Rechtsgrundlagen für den Einsatz biometrischer Fernidentifizierungssysteme im öffentlichen Raum geschaffen werden. Ein **Formulierungsvorschlag** ist der Stellungnahme beigefügt.

B. Beschränkung des Auskunftsanspruchs durch § 34 Abs. 1 Satz 2 BDSG-E und § 83 Abs. 1 Satz 2 SGB X-E

Durch einen neuen Satz 2 soll sowohl in § 34 Abs. 1 Satz 2 BDSG als auch in § 83 Abs. 1 Satz 2 SGB X eine neue Ausnahme für Auskunftsansprüche eingeführt werden. Demnach soll das Recht auf Auskunft auch insoweit nicht bestehen, als der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt.

Diese Neuerung stellt eine **Verschlechterung für die Betroffenenrechte** dar. Es ist zu befürchten, dass damit ein Ausnahmetatbestand geschaffen wird, der von Verantwortlichen zum einen übermäßig in Anspruch genommen wird und zum anderen für Betroffene, die ihre Interessen darlegen müssen, mit erheblichem Aufwand verbunden ist. Da Auskunftsansprüche oft der erste Schritt sind, um Rechtsschutz gegen unzulässige Datenverarbeitungen zu ergreifen, werden damit mittelbar die Rechtsschutzmöglichkeiten geschmälert.

Der Normtext insinuiert außerdem, dass bei Vorliegen der Voraussetzungen die Ausnahme absolut gelten soll, also auch keine teilweise Beschränkung der Auskunft möglich sein soll. Dem steht insbesondere ErwGr. 63 der Verordnung (EU) 2016/679 (im Folgenden „DSGVO“) entgegen,

demgemäß Ausnahmen nicht dazu führen dürfen, dass der betroffenen Person jegliche Auskunft verweigert wird. Außerdem trägt bereits Art. 15 Abs. 4 DSGVO dem Schutz von Geschäfts- und Betriebsgeheimnissen Rechnung, sodass sich die Farge stellt, inwiefern die Neuregelung überhaupt erforderlich ist.

C. Institutionalisierung der Datenschutzkonferenz

§ 16a BDSG-E ist im Grundsatz zu begrüßen, da er einen Schritt in Richtung Institutionalisierung der DSK darstellt, die auch im Koalitionsvertrag enthalten ist.[1] Dort ist auch vorgesehen, rechtlich, wo möglich, verbindliche Beschlüsse zu ermöglichen.[2] Allerdings bleibt § 16a BDSG-E dahinter zurück und verankert lediglich den status-quo der DSK im BDSG. Sie gibt derzeit bereits Auslegungshilfen, Leitlinien oder Empfehlungen zu Voraussetzungen und Rechtsfolgen einschließlich allgemeiner Einschätzungen zur Vereinbarkeit von konkretisierten Datenverarbeitungen mit dem Datenschutzrecht heraus, die aber nicht verbindlich sind.

Um Einheitlichkeit und Rechtssicherheit bei der Auslegung datenschutzrechtlicher Normen künftig wirksam zu ermöglichen, könnte eine Befugnis aufgenommen werden, die es der DSK erlaubt, **verbindlich Beschlüsse** zu fassen. Die Verbindlichkeit könnte auch beschränkt werden auf das Innenverhältnis und ggf. den nicht-öffentlichen Aufsichtsbereich. Die Einrichtung einer **Geschäftsstelle** könnte darüber hinaus dazu beitragen, die Arbeit der DSK durch einen administrativen Unterbau effizienter zu gestalten. Mit Blick auf das Verfassungsrecht stellt sich dabei vor allem die Frage, ob es sich um eine zulässige Form der sogenannten Mischverwaltung[3] handelt. Es gibt überzeugende rechtliche Gründe, dass bei einer derartigen Institutionalisierung weder Unions- noch Verfassungsrecht verletzt wird, da die Mischverwaltung dadurch gerechtfertigt werde könne, dass mit dem europarechtlich überformten Gebot eines effektiven und vereinheitlichten Vollzugs des Datenschutzrechts zur Behebung bestehender Vollzugsdefizite ein besonderer Sachgrund vorliege und die Datenschutzkonferenz zudem im Rahmen einer eng umgrenzten Sachmaterie tätig sei.[4] Dennoch sind damit einige verfassungsrechtliche Unsicherheiten verbunden, die, auch wenn eine Stärkung der Kooperation

[1] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter https://cms.gruene.de/uploads/assets/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf, S. 17.
[2] Ebd.
[3] Dazu z.B. *Ibler*, in: Dürig/Herzog/Scholz, 103. EL Januar 2024, GG Art. 87 Rn. 195 f.; *F. Kirchhof*, in: Dürig/Herzog/Scholz/, 103. EL Januar 2024, GG Art. 83 Rn. 117 ff.
[4] *Richter/Spiecker*, Rechtliche Möglichkeiten zur Stärkung und Institutionalisierung der Kooperation der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK 2.0), Rechtsgutachten im Auftrag der AG DSK 2.0, Januar 2022, insb. S. 25 ff.

in Form gemeinsamer und verbindlicher Entscheidungen begrüßenswert ist, eingepreist werden müssen. Nichtsdestotrotz dürften die damit verbundenen Vorteile dafür sprechen, diese Unsicherheiten in Kauf zu nehmen.

D. Aufnahme eines Verbots biometrischer Fernidentifikation im öffentlichen Raum in das BDSG

Biometrische Fernidentifikation stellt eine besondere Gefahr für Grund- und Menschenrechte dar (I). Die Reformbestrebungen des BDSG sollten deshalb genutzt werden, um ein Verbot biometrischer Fernidentifikation im öffentlichen Raum im BDSG zu verankern (II). Das Verbot sollte dabei möglichst weitreichend gefasst werden (III).

I. Biometrische Fernidentifikation als Gefahr für die Grundrechte

Biometrische Fernidentifikation im öffentlichen Raum birgt erhebliche Risiken und Gefahren für die Verwirklichung und den Schutz von Grund- und Menschenrechten.

Dass biometrische Daten besonders schutzwürdig sind, ergibt sich aus der besonderen Nähe biometrischer Daten zur Individualität und Identifizierbarkeit einer Person. Normativ ist diese grundsätzliche Wertung zum Bespiel in Art. 9 Abs. 1 DSGVO und Art. 10 Richtlinie (EU) 2016/680 (im Folgenden „JI-RL") sowie in § 48 BDSG verankert und wurde auch vom Bundesverfassungsgericht besonders hervorgehoben.[5]

Der Einsatz derartiger Technologie im öffentlichen Raum birgt das Risiko ausufernder Massenüberwachung. Personen können immer und überall eindeutig identifiziert werden. Dadurch können umfassende **Bewegungs- und Persönlichkeitsprofile** erstellt werden. Denn der Kontext des Aufenthaltsortes ermöglicht auch Rückschlüsse auf höchstpersönliche Daten, wie beispielsweise auf politische Einstellungen, die sexuelle Orientierung oder auch den Gesundheitszustand einer Person. Anonymität im öffentlichen Raum droht sowohl gegenüber staatlichen Stellen als auch gegenüber Privaten verloren zu gehen.

Diese Risiken haben erhebliche Auswirkungen auf das Verhalten von Menschen im öffentlichen Raum. Der Einsatz biometrischer Fernidentifikation ist mit enormen Abschreckungseffekten verbunden. Menschen können hierdurch von der Ausübung ihrer Grundrechte, insbesondere der

[5] BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 53: „höchstpersönliche Merkmale wie das Gesicht"; vgl. auch BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 87.

Meinungs- und Versammlungsfreiheit abgeschreckt werden (sog. **chilling effects**[6]), wenn sie befürchten, dabei jederzeit identifiziert werden zu können, auch wenn sie sich gesetzestreu verhalten.[7]

Hinzukommt, dass diese Instrumente der biometrischen Fernidentifikation höchst **fehleranfällig** sind.[8] In Bezug auf Gesichtserkennungssysteme kann festgestellt werden, dass nicht weiße Menschen, aber auch non-binäre und transgender Personen besonders häufig falsch identifiziert werden und in der Folge illegitimen, grundrechtsbeschränkenden Maßnahmen ausgesetzt sind. Das haben inzwischen verschiedene Studien gezeigt.[9] Die Nutzung fehleranfälliger Systeme greift nicht nur erheblich in Grundrechte unbescholtener Menschen ein, sondern dürfte somit auch nicht den Ansprüchen an die Effektivität polizeilicher Arbeit gerecht werden. So führte fehlende Effektivität auch in Sachsen dazu, dass die 2019 geschaffene Rechtsgrundlage, die den Einsatz biometrischer Fernidentifikationssystemen im öffentlichen Raum legitimieren sollte, bereits nach ihrer ersten gesetzlich vorgesehenen Evaluation nicht verlängert wurde.[10]

Auch **strukturelle Diskriminierung** – insbesondere struktureller Rassismus – wird durch den Einsatz solcher Systeme verstärkt. Vor allem dann, wenn Referenzdatenbanken aus polizeilichen Datenbanken bestehen, setzen sich die darin angelegten Diskriminierungen fort. Das Risiko von weiteren polizeilichen Maßnahmen betroffen zu sein, ist somit für marginalisierte Gruppen deutlich höher.

Da biometrische Daten anders als beispielsweise Kreditkartennummern oder Passwörter nicht geändert werden können, aber oft als Authentifizierungsinstrument genutzt werden, kann es zu

---

[6] *Assion*, Überwachung und Chilling Effects, in: Überwachung und Recht. Tagungsband zur Telemedicus Sommerkonferenz, 2014, S. 31 ff.; vgl. auch BVerfG, Beschluss v. 17.02.2009, 1 BvR 2492/08, Rn. 131.

[7] Dazu ausführlich z.B. International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, S. 14 f., abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Facial-Recognition-Tech-EN.pdf?__blob=publicationFile&v=2.

[8] *Hälterlein*, Biometrische Gesichtserkennung – technologischer Solutionismus für mehr „Sicherheit", 8. April 2024, abrufbar unter https://www.cilip.de/2024/04/08/biometrische-gesichtserkennung-technologischer-solutionismus-fuer-mehr-sicherheit/; zur Trefferquote beim Pilotprojekt „Südkreuz": *Chaos Computer Club*, Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, 13. Oktober 2018, abrufbar unter https://www.ccc.de/en/updates/2018/debakel-am-suedkreuz.

[9] Z.B. *Buolamwini/Gebru*, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, in: Proceedings of Machine Learning Research, Vol. 81, 2018, S. 77-91; International Working Group on Data Protection in Technology, Working Paper on Facial Recognition Technology, S. 15 ff. m.w.N., abrufbar unter https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20230608_WP-Facial-Recognition-Tech-EN.pdf?__blob=publicationFile&v=2.

[10] Pressemitteilung des Sächsischen Staatsministerium des Innern v. 22. August 2023, abrufbar unter https://www.medienservice.sachsen.de/medien/news/1068787.

erheblichen Konsequenzen führen, wenn unberechtigte Zugriffe auf biometrische Datenbanken stattfinden. Dieses Risiko besteht sowohl für die private als auch die staatliche Nutzung. Die Verwendung von biometrischen Fernidentifikationssystemen würde tendenziell dazu führen, dass biometrische Datenbanken entstehen oder vergrößert werden. Mit dem Einsatz gehen somit erhebliche Risiken der **Datensicherheit** einher.

Nicht zuletzt aufgrund der enormen **Streubreite** biometrischer Fernidentifikation handelt es sich um schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Betroffen sind alle Personen, deren biometrische Daten abgeglichen werden. Das Bundesverfassungsgericht hat klargestellt, dass auch Nicht-Treffer Eingriffe in die Grundrechte der Personen, deren Daten abgeglichen werden, darstellen.[11] Dadurch, dass die Maßnahme heimlich stattfindet, verschärft sich der Eingriff, da Rechtsschutzmöglichkeiten für Betroffene dann regelmäßig nur sehr eingeschränkt möglich sind.[12]

II. Umsetzung eines Verbots im BDSG

Bereits in der Anhörung im Digitalausschuss zum Thema „Nationale Spielräume bei der Umsetzung des europäischen Gesetzes über Künstliche Intelligenz" am 15. Mai 2024 wurde die Möglichkeit, ein Verbot in das BDSG aufzunehmen thematisiert.[13]

Die Verankerung eines Verbots biometrischer Fernidentifikation im öffentlichen Raum in das BDSG ist angesichts der aktuellen Rechtslage und Praxis erforderlich, um den Koalitionsvertrag umzusetzen (1). Sowohl das Unionsrecht (2) als auch die nationale verfassungsrechtliche Kompetenzordnung (3) ermöglichen die Umsetzung eines Verbots im BDSG. Auch der Anwendungsbereich und die Auswirkungen eines Verbots im BDSG sprechen dafür, ein Verbot dort zu verankern (4).

1. Notwendigkeit gesetzgeberischer Klarstellung und Umsetzung des Koalitionsvertrags

Durch die **KI-Verordnung** (im Folgenden „KI-VO") selbst wird gem. Art. 5 Abs. 1 lit. h KI-VO nur ein kleiner Teil der biometrischen Fernidentifizierung im öffentlichen Raum verboten. Dieser betrifft die Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich

[11] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, Rn. 51.
[12] BVerfG, Urteil des Ersten Senats vom 11. März 2008, 1 BvR 2074/05, 1 BvR 1254/07, Rn. 79.
[13] *Roth-Isigkeit*, Stellungnahme im Rahmen der öffentlichen mündlichen Anhörung am 15. Mai 2024 des Digitalausschusses des Bundestags zum Thema Nationale Spielräume bei der Umsetzung des europäischen Gesetzes über künstliche Intelligenz, 15. Mai 2023, S. 27 f., abrufbar unter https://www.bundestag.de/resource/blob/1002542/9399017597afda26d626a23617a30bbb/Roth-Isigkeit.pdf.

zugänglichen Räumen zu Zwecken der Strafverfolgung und gilt auch nicht absolut, sondern sieht eine Reihe von Ausnahmen vor. Das Verbot betrifft damit „nur" die Strafverfolgung, wobei darunter nach Art. 3 Abs. 46 KI-VO auch die Abwehr von Gefahren für die öffentliche Sicherheit gehört.

Derzeit existieren für nationale **Polizei- und Sicherheitsbehörden** im Bereich der Strafverfolgung und Gefahrenabwehr keine spezifischen Rechtsgrundlagen, die den Einsatz biometrischer Fernidentifikation erlauben[14], sodass die Verwendung derzeit rechtswidrig wäre. Die KI-Verordnung stellt zwar Anforderungen an diese Systeme und potenzielle Befugnisnormen, beinhaltet selbst aber keine Rechtsgrundlagen, die staatliche Eingriffe durch biometrische Fernidentifikationssysteme legitimieren. Nichtsdestotrotz hat sich jüngst durch die mediale Berichterstattung[15] sowie kleine Anfragen in verschiedenen Landesparlamenten[16] gezeigt, dass solche Systeme bereits im Einsatz sind. Der Bundesgesetzgeber sollte deshalb unbedingt durch ein Verbot klarstellen, dass der Einsatz dieser Systeme nicht erlaubt ist.

Mit Blick auf das Verbot des Image-Scrapings in Art. 5 Abs. 1 lit. e KI-VO sind die Möglichkeiten **Privater** beim Einsatz von Systemen biometrischer Gesichtserkennung zwar teilweise schon beschränkt. Demnach ist es nicht erlaubt, ungezielt Gesichtsbilder aus dem Internet oder aus Videoüberwachungsaufnahmen auszulesen. Damit dürfte zwar die Nutzung von Systemen wie PimEyes oder Clearview schon nach der KI-VO eindeutig unzulässig sein. Ein umfassender, lückenloser Ausschluss biometrischer Fernidentifikation durch Private ist dadurch aber nicht sichergestellt. Denn Fernidentifikation kann nicht nur über den Abgleich von Gesichtsbildern, sondern auch mittels anderer physischer, physiologischer und verhaltensbezogener menschlicher Merkmale erfolgen, wie Augenbewegungen, Körperform, Stimme, Prosodie, Gang, Haltung, Herzfrequenz, Blutdruck, Geruch oder charakteristischer Tastenanschlag (vgl. ErwGr. 15

[14] Die Eingriffe werden z.B. auf §§ 163f, 100h StPO i.V.m. § 98a StPO gestützt, also einer Kombination aus Ermittlungsvorschriften, die weder für sich noch in Kombination Rechtsgrundlagen für den Einsatz biometrischer Fernidentifikationssysteme darstellen können, da sie vor dem Hintergrund des verfassungsrechtlichen Bestimmtheitsgrundsatzes weder den Einsatz dieser Systeme spezifisch adressieren noch die verfassungsrechtlichen Voraussetzungen an derart erhebliche Eingriffe in die informationelle Selbstbestimmung erfüllen. Auch § 98c StPO sowie § 48 BDSD erlauben nur geringfügige Eingriffe und können für die biometrische Fernidentifizierung deshalb nicht herangezogen werden.

[15] Z.B. *Monroy*, Polizei observiert mit Gesichtserkennung, netzpolitik.org v. 3 Mai 2024, abrufbar unter https://netzpolitik.org/2024/ueberwachungstechnik-polizei-observiert-mit-gesichtserkennung/; *Krempl*, Gesichtserkennung: Datenschutzaufsicht Niedersachsen prüft heimliche Observation, heise online v. 15 Juni 2024, abrufbar unter https://www.heise.de/news/Gesichtserkennung-Datenschutzaufsicht-Niedersachsen-prueft-heimliche-Observation-9764663.html?wt_mc=nl.red.ho.ho-nl-daily.2024-06-17.ansprache.ansprache.

[16] Z.B. Berlin: Drs. 19/18874, Drs. 19/18461; Sachsen: Drs. 7/16310, Drs. 7/16308.

KI-VO). Abgesehen davon bleibt auch das gezielte Auslesen von Gesichtsbildern weiterhin möglich und kann Grundlage für die Erstellung von Referenzdatenbanken sein.

Im Anwendungsbereich der **DSGVO** ist die Verarbeitung biometrischer Daten unter bestimmten Voraussetzungen möglich, sodass auch hier Rechtsunsicherheiten und etwaige Lücken durch ein eindeutiges Verbot, das Private als auch öffentliche Stellen betrifft, geschlossen werden sollten. Art. 9 Abs. 1 DSGVO untersagt zwar grundsätzlich die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person. Es bestehen aber nach Art. 9 Abs. 2 DSGVO Ausnahmen von diesem Verbot, die auch Spielräume für die Konkretisierung durch die Mitgliedstaaten eröffnen, die teilweise durch Fachgesetzte, aber auch durch § 22 BDSG ausgefüllt werden.[17]

Auch wenn zweifelhaft ist, ob es überhaupt Einzelfälle gibt, bei denen Private biometrische Fernidentifikation nach den Vorschriften der DSGVO einsetzen dürften, ist es angesichts der Ausnahmemöglichkeiten zu Art. 9 DSGVO erforderlich, etwaige Lücken zu schließen und auch den Einsatz durch nichtöffentliche Stellen zu verbieten.

Darüber hinaus hat sich die Bundesregierung im **Koalitionsvertrag** klar gegen den Einsatz von biometrischer Erfassung zu Überwachungszwecken ausgesprochen. Das Recht auf Anonymität sowohl im öffentlichen Raum als auch im Internet sei zu gewährleisten.[18] Ein entsprechendes Verbot im BDSG zu verankern, würde dieses Versprechen bekräftigen.

2. Unionsrechtlicher Rahmen

Ein Verbot ist nach **Art. 9 Abs. 4 DSGVO** unbedenklich, der es den Mitgliedstaaten erlaubt, zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrechtzuerhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Auch die **JI-Richtlinie** gibt hinsichtlich der Verarbeitung biometrischer Daten nach Art. 10 JI-RL nur Mindeststandards vor (vgl. Art. 1 Abs. 3 JI-RL) und stünde einem Verbot nicht entgegen.

Ebenso erlaubt die **KI-VO** nationale Verbotsregelungen einzuführen: Für die Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen können die Mitgliedstaaten nach Art. 5

[17] Vgl. *Albers/Veit*, in: BeckOK DatenschutzR, 48. Ed. 1.5.2024, BDSG § 22 Rn. 15.
[18] Mehr Fortschritt wagen, Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit, Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, abrufbar unter https://cms.gruene.de/uploads/assets/Koalitionsvertrag-SPD-GRUENE-FDP-2021-2025.pdf, S. 86.

Abs. 5 Satz 5 KI-VO im Einklang mit dem Unionsrecht restriktivere Rechtsvorschriften für den Einsatz biometrischer Fernidentifizierungssysteme erlassen. Damit wäre auch ein vollständiges Verbot möglich. Gem. Art. 26 Abs. 10 UAbs. 7 KI-VO können die Mitgliedstaaten im Einklang mit dem Unionsrecht strengere Rechtsvorschriften für die Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung erlassen, sodass auch für die retrograde Fernidentifikation eine nationale Verbotsvorschrift möglich ist. Da die KI-VO an vielen Stellen Bezug auf das unionsrechtliche Datenschutzrecht nimmt und dieses grundsätzlich unberührt lässt (Art. 2 Ab.s 7 KI-VO), bietet es sich an, diesen Ansatz auch in der nationalen Umsetzung aufzugreifen und die Verbote im BDSG zu verorten.

3. Gesetzgebungskompetenzen

Ein Verbot biometrischer Fernidentifizierung ist für die dem Bundesgesetzgeber innerhalb der ihm durch das Grundgesetz kompetenzrechtlich zugewiesenen Regelungsmaterien möglich.

Da sich das Datenschutzrecht als eine **Querschnittsmaterie** darstellt, ergibt sich die Gesetzgebungskompetenz des Bundes als Annex aus verschiedenen Sachkompetenzen der Art. 73 und 74 GG.[19] Die Kompetenz für den Bund zur Regelung des Datenschutzrechts ergibt sich also aus seiner jeweiligen Zuständigkeit für bestimmte Sachbereiche, in deren Rahmen Daten verarbeitet werden, also beispielsweise für das Strafrecht aus Art. 74 Abs. 1 Nr. 1, 72 GG oder den Zoll- und Grenzschutz aus Art. 73 Abs. 1 Nr. 5 GG. Die datenschutzrechtliche Regelungskompetenz des Bundesgesetzgebers für nichtöffentliche Stellen kann als Annexkompetenz auf Art. 74 Abs. 1 Nr. 1, 11 und 12 GG gestützt werden.[20] Für die Gefahrenabwehr der Länder ist der Bund hingegen nicht kompetent, sodass es den Landesgesetzgebern obliegt, entsprechende Verbotsnormen vorzusehen.

4. Anwendungsbereich und Wirkung des BDSG

Auch mit Blick auf den Anwendungsbereich und potenzielle Auswirkungen im Zusammenspiel mit anderen Gesetzen erscheint die Verankerung eines Verbots biometrischer Fernidentifikation im BDSG sinnvoll.

Für **nichtöffentliche Stellen** ergibt sich der Anwendungsbereich recht unproblematisch aus § 1 Abs. 1 Satz 2 BDSG. Gem. § 1 Abs. 1 Satz 1 Nr. 1 BDSG gelten die Regelungen des BDSG für **öffentliche**

[19] *Sydow*, in: Sydow/Marsch, DS-GVO/BDSG, 3. Aufl. 2022, Einleitung Rn. 92.
[20] Vgl. *Sydow*, in: Sydow/Marsch, DS-GVO/BDSG, 3. Aufl. 2022, Einleitung Rn. 93; *Gusy/Eichenhofer*, in: BeckOK DatenschutzR, 48. Ed. 1.11.2021, BDSG § 1 Rn. 76; BT-Drs. 18/11325, S. 71.

Stellen des Bundes. Für **öffentliche Stellen der Länder** gilt das BDSG nur **subsidiär** (§ 1 Abs. 1 Satz 1 Nr. 2 BDSG): Existiert landesspezifisches Datenschutzrecht, hat dieses Vorrang. Das BDSG gilt aber dann („soweit"), wenn die Vorschriften des Landesdatenschutzrechts einen Sachverhalt nicht oder nicht abschließend regeln und die weiteren Voraussetzungen des § 1 Abs. 1 S. 1 Nr. 2 vorlegen.[21]

Zwar ist das BDSG subsidiär zu spezielleren **Fachgesetzen** (§ 1 Abs. 2 Satz 1 BDSG). Wenn die Fachgesetze einen Sachverhalt, für den das BDSG gilt, aber nicht oder nicht abschließend regeln, finden hingegen die Vorschriften des BDSG Anwendung (vgl. § 1 Abs. 2 Satz 2 BDSG). Das BDSG gilt also subsidiär als Auffanggesetz mit dem Ziel, im bereichsspezifischen Recht Datenschutzlücken zu füllen und datenschutzrechtsfreie Räume zu vermeiden.[22]

Eine Verankerung im BDSG bietet sich deshalb an, weil es vorliegend um ein **klarstellendes, die Fachgesetze übergreifendes** und damit kein bereichsspezifisches Verbot geht. Denkbar sind davon unabhängig auch ergänzende bereichsspezifische Verbote in den Fachgesetzen. Die Subsidiaritätsklausel ist unbedenklich, solange in den Fachgesetzen keine Befugnisse oder Regelungen existieren, die die biometrische Fernidentifikation im Sinne einer Tatbestandskongruenz[23] adressieren.

Besonders hervorzuheben ist § 500 StPO, der für das Strafprozessrecht den **Anwendungsbereich für die Länder nochmals erweitert**, indem er anordnet, dass Teil 3 des BDSG entsprechend anzuwenden ist, soweit öffentliche Stellen der Länder im Anwendungsbereich der StPO personenbezogene Daten verarbeiten (Abs. 1) und soweit in der StPO nicht etwas anderes bestimmt ist. Daraus folgt, dass StPO und BDSG miteinander verschränkt sind und für die Polizei im repressiven Bereich das BDSG gilt.[24] Die §§ 45 ff. BDSG bilden den „allgemeinen Teil", welcher durch spezifische Rechtsvorschriften in der StPO für das Strafverfahren ergänzt wird.[25]

III. Reichweite des Verbots

Es sollte ein umfassendes Verbot im BDSG verankert werden, um Grund- und Menschenrechte effektiv zu schützen. Das Verbot soll sich folglich an öffentliche Stellen und Private richten (1), die retrograde als auch die Echtzeit-Fernidentifizierung erfassen (2) sowie die Erhebung und die

[21] *Klar*, in: Kühling/Buchner, 4. Aufl. 2024, BDSG § 1 Rn. 9.
[22] *Gusy/Eichenhofer*, in: BeckOK DatenschutzR, 48. Ed. 1.11.2021, BDSG § 1 Rn. 81.
[23] *Gola/Reif*, in: Gola/Heckmann, 3. Aufl. 2022, BDSG § 1 Rn. 10.
[24] *Singelnstein*, NStZ 2020, 639 (639).
[25] *Braun*, in: Gola/Heckmann, 3. Aufl. 2022, BDSG § 45 Rn. 4.

Weiterverarbeitung betreffen (3). Dies ließe sich konkret in bereits bestehende Normen des BDSG integrieren (4).

1. Öffentliche Stellen und Private als Adressat*innen

Ein Verbot sollte in jedem Fall für öffentliche Stellen im Sinne des § 2 BDSG gelten, und zwar sowohl im Anwendungsbereich der DSGVO als auch der JI-RL. Darüber hinaus sollte aber auch für Private der Einsatz biometrischer Fernidentifikationssysteme verboten werden. Somit sollte der Gesetzgeber ein Verbot sowohl in **Teil 2 als auch in Teil 3 des BDSG** verankern.

2. Retrograd und Echtzeit

Das Verbot sollte sowohl die biometrische Echtzeit-Fernidentifizierung als auch die retrograde biometrische Fernidentifizierung erfassen.

Zwar stellt EWG 32 der KI-VO darauf ab, dass mit der biometrischen Echtzeit-Fernidentifikation einige spezifische Risiken einhergehen, die sich aus der Unmittelbarkeit der Auswirkungen und den begrenzten Möglichkeiten weiterer Kontrollen oder Korrekturen ergeben. Dass bei einem Live-Abgleich der Aufenthaltsort einer Person bestimmt und auf die Person damit unmittelbar zugegriffen werden kann, mag ein spezifisches Echtzeit-Risiko zu sein. Allerdings birgt auch der **retrograde Abgleich spezifische Risiken**, sodass die retrograde Fernidentifikation nicht per se weniger eingriffsintensiv ist. Während Echtzeit Fernidentifikation punktuell eingriffsintensiv ist, ermöglichen es retrograde Abgleiche, über einen langen Zeitraum hinweg besonders verdichtete Bewegungs- und Persönlichkeitsprofile zu erstellen. Er schafft Anreize für lange Speicherfristen und Einschüchterungseffekte vertiefen sich, wenn Videomaterial auf unabsehbare Zeit in der Zukunft auswertbar ist. Hinzu kommt, dass auch ein retrograder Abgleich, anders als der Erwägungsgrund suggeriert, technisch zunächst keine Kontrollen und Korrekturen voraussetzt. Dabei handelt es sich vielmehr um Fragen der konkreten Ausgestaltung des Verfahrens in etwaigen gesetzlichen Ermächtigungsgrundlagen. Darüber hinaus betreffen die oben (B.I) dargestellten Risiken und Gefahren gerade jede Form der biometrischen Fernidentifikation und sind nicht prinzipiell reduziert, wenn der Abgleich später erfolgt. Denn das Risiko einer ausufernden Massenüberwachung, der Erstellung umfassender Bewegungs- und Persönlichkeitsprofile, einhergehende Einschüchterungseffekte, das Diskriminierungspotenzial und die Streubreite betreffen die Verwendung biometrischer Fernidentifikationssysteme insgesamt.

Maßgeblich für die Beurteilung des konkreten Eingriffsgewichts einer Maßnahme sind nach verfassungsgerichtlicher Rechtsprechung vielmehr andere Faktoren. Dazu gehören Art, Umfang

und denkbare Verwendung der Daten, die Gefahr ihres Missbrauchs, die Anzahl der betroffenen Grundrechtsträger*innen, die Intensität der Beeinträchtigungen und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben, ob eine Maßnahme heimlich stattfindet und wie die Rechtsschutzmöglichkeiten ausgestaltet sind.[26] Auch die Fehler- und Diskriminierungsanfälligkeit spielt dafür eine Rolle.[27]

3. Erhebung und Weiterverarbeitung

Neben einem Erhebungsverbot durch biometrische Fernidentifizierungssysteme sollten auch Weiterverarbeitungsverbote in das BDSG aufgenommen werden.

Da ein Erhebungsverbot im BDSG außerhalb des Anwendungsbereichs keine Wirkung entfaltet, ist es nicht ausgeschlossen, dass auf Landesebene zum Beispiel Rechtsgrundlagen in den jeweiligen Polizeigesetzen geschaffen werden. Diese könnten die dadurch erhobenen Daten an Bundesbehörden übermitteln bzw. selbst in Ermittlungsverfahren, also repressiv, nutzen wollen. § 161 Abs. 3 Satz 1 StPO schränkt lediglich die Verwertung derart erhobener Daten zu Beweiszwecken ein, steht aber einer Verwendung als Spurenansatz oder als Anlass eines Anfangsverdachts nicht entgegen.[28] Ein spezielles Weiterverarbeitungsverbot im BDSG für Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme in öffentlich zugänglichen Räumen aufgrund anderer Gesetze erhoben wurden, könnte eine Verwendung abseits der Verwertung zu Beweiszwecken verhindern, auch wenn sich die spezielle Vorschrift dann im „allgemeineren" Gesetz, nämlich im BDSG befinden würde.

4. Formulierungsvorschlag

Es wird vorgeschlagen, Erhebungs- und Weiterverarbeitungsverbote in die Normen des BDSG zu integrieren, die die Verarbeitung biometrischer Daten betreffen. Es sollte sichergestellt sein, dass die Begrifflichkeiten denen in der DSGVO, JI-RL und KI-VO entsprechen und einheitlich verwendet werden. Gegebenenfalls reicht auch ein Hinweis auf die Definitionen der verwendeten Begriffe in der Gesetzesbegründung aus. Jedenfalls sollte in der Gesetzesbegründung explizit darauf verwiesen werden, dass die Verbote zur Weiterverwendung auch im Rahmen in

[26] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 76 m.w.N.
[27] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 90.
[28] Vgl. *Kölbel/Ibold*, in: MüKoStPO, 2. Aufl. 2024, StPO § 161 Rn. 45; BVerfG, Beschluss der 3. Kammer des Zweiten Senats vom 29. Juni 2005, 2 BvR 866/05, Rn. 4.

repressiven Ermittlungsverfahren gelten und insofern neben § 161 Abs. 3 StPO treten, indem sie auch die Verwendung als Spurenansatz verbieten.

In **§ 22 BDSG** könnte folgender neuer Absatz 3 eingefügt werden:

„(3) Die Verarbeitung personenbezogener Daten durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) ist unzulässig."

In **§ 23 BDSG** könnte folgender neuer Satz 2 in Abs. 2 eingefügt werden:

„Die Verarbeitung personenbezogener Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) aufgrund anderer Gesetze erhoben wurden, ist unzulässig."

In **§ 24 BDSG** könnte folgender neuer Satz 2 in Abs. 2 eingefügt werden:

„Die Verarbeitung personenbezogener Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) aufgrund anderer Gesetze erhoben wurden, ist unzulässig."

In **§ 48 BDSG** könnte folgender neuer Absatz 3 eingefügt werden:

„(3) Die Verarbeitung personenbezogener Daten durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) ist unzulässig."

In **§ 49 BDSG** könnte folgender neuer Satz 3 eingefügt werden:

„Die Verarbeitung personenbezogener Daten, die durch die Verwendung biometrischer Fernidentifizierungssysteme (Art. 3 Nr. 41 KI-VO) in öffentlich zugänglichen Räumen (Art. 3 Nr. 44 KI-VO) aufgrund anderer Gesetze erhoben wurden, ist unzulässig."