PRIGGE
IT MEDIEN
RECHT

Prigge Recht Sternstraße 58 40479 Düsseldorf

Dr. Jasper Prigge, LL.M.
Rechtsanwalt
Fachanwalt für Urheber- und Medienrecht
Fachanwalt für IT-Recht

[redacted]

Verwaltungsgericht Frankfurt am Main
Adalbertstraße 18
60486 Frankfurt

Ihr Zeichen	**Unser Zeichen**	**Datum**
5 K 6427/25.F	[redacted]	22.04.2026

In dem Rechtsstreit

[redacted] **. Land Hessen**

begründen wir die Klage ergänzend wie folgt:

Prigge Recht
Rechtsanwalt Dr. Jasper Prigge
Sternstraße 58
40479 Düsseldorf

Tel 0211 417 4899-0
Mail kontakt@prigge-recht.de
Web www.prigge-recht.de

[redacted]

Inhaltsverzeichnis

I. Zusammenfassung

Vor der ausführlichen Begründung fassen wir die maßgeblichen Punkte des Rechtsstreits wie folgt zusammen:

Die Ermächtigungsgrundlage in § 14 Abs. 9 - 11 HSOG ist verfassungswidrig. Die Norm genügt nicht dem Gebot der Normenbestimmtheit und Normenklarheit, da sie weder hinreichend bestimmte Eingriffsschwellen noch verbindliche Vorgaben zur Festlegung der Mindestähnlichkeitsschwelle enthält. Sie ist unverhältnismäßig, weil sie Eingriffe ohne das Vorliegen einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter zulässt und verfassungsrechtlich gebotene Verfahrensvorschriften — insbesondere Löschpflichten, Benachrichtigungspflichten, Berichtspflichten und Softwaremonitoring — fehlen.

Darüber hinaus verletzen die auf § 14 Abs. 9–11 HSOG gestützten Maßnahmen auch im konkreten Einzelfall das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und das Grundrecht auf Vereinigungsfreiheit aus Art. 9 Abs. 1 GG der Kläger:innen. Die Maßnahme trifft die Kläger:innen auch in ihrer Eigenschaft als Vorstandsmitglieder einer Beratungsstelle, dessen Funktionsfähigkeit durch die Abschreckungs- und Einschüchterungseffekte auf ihre Klient:innen strukturell gefährdet wird. Dem besonders hohen Eingriffsgewicht steht kein hinreichend gewichtiger Rechtsgutsschutz gegenüber.

Die Maßnahme verstößt schließlich gegen Unionsrecht. § 14 Abs. 9–11 HSOG enthält keine hinreichend detaillierten Vorschriften für die menschliche Aufsicht und Berichterstattung nach Art. 5 KI-VO. Auch die Eilbefugnis nach § 14 Abs. 11 S. 2 HSOG unterschreitet unionsrechtlichen Anforderungen.

II. Zulässigkeit

Die Klage ist zulässig.

1. Klagebefugnis

Die Kläger:innen sind klagebefugt. Die biometrische Echtzeit-Fernidentifizierung nach § 14 Abs. 9 – 11 HSOG stellt eine schwerwiegende Verletzung des Grundrechts der Kläger:innen auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG dar.

Das Recht auf informationelle Selbstbestimmung umfasst das Recht, selbst darüber zu entscheiden, wann und wem man personenbezogene Daten offenbart.

> *Barczak*. in: Dreier, GG-Kommentar, 4. Aufl. 2023, Art. 2 I GG Rn. 90.

Gem. Art. 4 Nr. 1 DSGVO sind personenbezogene Daten solche Daten, die sich auf eine identifizierbare natürliche Person beziehen. Dazu zählen Gesichter und Gesichtszüge als besondere physiologische Merkmale einer Person. Im vorliegenden Fall werden beim Einsatz der Maßnahme nach § 14 Abs. 9 – 11 HSOG die Gesichtszüge aller sich im Sichtfeld der Kamera befindlichen Personen und somit auch die der Kläger:innen erfasst, gespeichert und mit denen der gesuchten Person abgeglichen.

2. Rechtsschutzbedürfnis

Das Rechtsschutzbedürfnis der Kläger:innen ist maßgeblich dadurch begründet, dass bei der Verletzung des Rechts auf informationelle Selbstbestimmung Wiederholungsgefahr besteht. Es ist mit hinreichender Wahrscheinlichkeit davon auszugehen, dass die Kläger:innen seit Beginn des polizeilichen Pilotprojekts im Juli 2025 sowie auch in Zukunft durch Maßnahmen nach § 14 Abs. 9 – 11 HSOG betroffen waren bzw. sein werden. Insbesondere kann ohne Weiteres angenommen werden, dass weitere Eingriffe drohen, wenn bereits eine Beeinträchtigung stattgefunden hat,

> vgl. BVerwG, Urteil vom 25. Januar 2012 - 6 C 9/11, NVwZ 2012, 757 (758 Rn. 21).

Eine der mit der Software zur biometrischen Echtzeit-Fernidentifizierung verknüpften Kamera erfasst den Eingangsbereich der Beratungsstelle des Vereins Doña Carmen e.V. Darüber hinaus erfasst das Sichtfeld einer zweiten Kamera die anliegende Kreuzung; die restlichen drei befinden sich eine bis zwei Straßenkreuzungen weiter,

vgl. Anlage B4.

Als Vorstandsmitglieder des Vereins halten sie sich wöchentlich [redacted] in den Räumlichkeiten auf, [redacted]. Da sie dadurch regelmäßig auf ihrem Arbeitsweg sowie konkret beim Betreten und Verlassen der Räumlichkeiten das Sichtfeld von mindestens einer der Kameras durchqueren, besteht eine hohe Wahrscheinlichkeit, dass sie auch in Zukunft beim Einsatz der biometrischen Echtzeit-Fernidentifizierung nach § 14 Abs. 9 – 11 HSOG von der Kamera (mit-)erfasst und ihre biometrischen Daten zum Abgleich mit der jeweils gesuchten Person abgeglichen werden.

Die Wiederholungsgefahr wird zudem durch die bisherige Einsatzpraxis untermauert: Nach den Ausführungen des Beklagten (Schriftsatz vom 16. März 2026, S. 4) wurden im Zeitraum vom 10. Juli 2025 bis zum 28. Februar 2026 14 Beschlussanträge durch die Polizei bei Gericht eingereicht; in acht Fällen wurde die Maßnahme tatsächlich durchgeführt. Die konkrete Dauer des jeweiligen Einsatzes ist unbekannt; in der Datenschutzfolgenabschätzung wird jedoch von einem zulässigen Anordnungszeitraum bis zu drei Monaten ausgegangen, der bei Folgeanträgen ggf. verlängert werden könne,

vgl. DSFA, Anlage B7, S. 43.

Angesichts dieser Einsatzhäufigkeit und möglichen Durchführungsdauer sowie der regelmäßigen Präsenz der Kläger:innen im Kamerasichtfeld besteht eine hohe Warscheinlichkeit, dass sie bereits im Rahmen vergangener Maßnahmen erfasst wurden. Selbst wenn dies nicht abschließend feststellbar ist, begründet die dokumentierte Einsatzfrequenz jedenfalls eine hinreichend konkrete Gefahr künftiger Betroffenheit.

Darüber hinaus begründet auch die Heimlichkeit des Eingriffs ein Rechtsschutzbedürfnis der Kläger:innen, da, nachgelagerter Rechtsschutz gegen die Erfassung ihrer biometrischen Merkmale sowie den anschließenden Datenabgleich nicht in Betracht kommt,

> vgl. VGH München, Urteil vom 17. Dezember 2012 - 10 BV 09.2641, BeckRS 2013, 49007, Rn. 60.

III. Begründetheit

Die Klage ist begründet, da die Anspruchsvoraussetzungen eines öffentlich-rechtlichen Unterlassungsanspruchs nach § 1004 BGB analog gegeben sind und als Rechtsfolge die Unterlassung der automatisierten Erfassung und Auswertung der biometrischen Daten der Kläger:innen verlangt werden kann.

Die Voraussetzungen eines vorbeugenden Unterlassungsanspruchs liegen vor. Der öffentlich-rechtliche Unterlassungsanspruch setzt die begründete Besorgnis voraus, der Beklagte werde künftig durch sein hoheitliches Handeln rechtswidrig in die geschützte Rechts- und Freiheitssphäre des Klägers eingreifen,

> vgl. BVerwG, Urteil vom 22. Oktober 2014 - 6 C 7/13 -, NVwZ 2015, 906 (907 Rn. 20).

Dies ist im vorliegenden Fall erfüllt, da durch die Anwendung der biometrischen Echtzeit-Fernidentifizierung nach § 14 Abs. 9 – 11 HSOG mit hinreichender Wahrscheinlichkeit ein rechtswidriger Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und das Grundrecht Vereinigungsfreiheit aus Art. 9 Abs. 1 GG droht.

1. Betroffenheit eines subjektiv-öffentlichen Rechts

Die Kläger:innen sind von der Maßnahme in ihren subjektiv-öffentlichen Rechten betroffen.

a) Grundrecht auf informationelle Selbstbestimmung

Der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist hier eröffnet. Es schützt das Recht jeder Person, selbst über die Preisgabe und Verwendung ihrer personenbezogenen Daten zu bestimmen,

> BVerfG, Urteil vom 15.12.1983 - 1 BvR 209/83 -, BVerfGE 65, 1 (43); *Di Fabio*, in: Dürig/Herzog/Scholz, Grundgesetz, 106. EL Oktober 2024, Art. 2 Rn. 175.

Damit stellt das Grundrecht eine Reaktion auf das Gefährdungspotential moderner Datenverarbeitung dar. Hierdurch sollen die essentiellen Bedingungen von Privatheit garantiert, die autonome Persönlichkeitsentwicklung vor illegitimen Einflüssen abgeschirmt und schließlich Verhaltensfreiheit ermöglicht werden,

> BVerfG, Beschluss vom 13.06.2007 - 1 BvR 1550/03 -, - 1 BvR 2357/04 -, - 1 BvR 603/05 -, NJW 2007, 2464 (2466); *Eichberger*, in: Huber/Voßkuhle, Grundgesetz, 8. Auflage 2024, Art. 2 Rn. 282.

Das BVerfG hat insoweit klargestellt, dass es aufgrund der technischen Verarbeitungsmöglichkeiten „kein belangloses Datum“ gibt,

> BVerfGE 65, 1 (45).

Grund dafür ist, dass auch Daten mit geringem Informationsgehalt in Verknüpfung mit anderen Daten Rückschlüsse auf den Betroffenen zulassen können,

> *Barczak*, in: Dreier, Grundgesetz-Kommentar, 4. Auflage 2023, Art. 2 Abs. 1 Rn. 92.

In Bezug auf den Einsatz von staatlichen Überwachungsmaßnahmen (wie denen des § 14 Abs. 9 – 11 HSOG) sind alle personenbezogenen Daten geschützt, die sich aus einer gespeicherten und abrufbaren oder einer Echtzeit-Aufnahme im öffentlichen Raum ablesen lassen,

> BVerfGE 65, 1 (43),

wie etwa der Aufenthalt an einem bestimmten Ort.

Die Kläger:innen befinden sich regelmäßig im Sichtfeld der Kamera (siehe dazu oben I.2.). Bei paralleler Aktivierung der Echtzeit-Fernidentifizierung werden ihre biometrischen Daten von der Kamera erfasst und automatisiert mit einem Vergleichsdatensatz abgeglichen.

b) Grundrecht auf Vereinigungfreiheit

Die Kläger:innen sind auch in ihrer Vereinigungsfreiheit betroffen. Art. 9 Abs. 1 GG gewährleistet allen Deutschen das Recht, Vereine und Gesellschaften zu bilden. Das Grundrecht schützt dabei nicht nur den Gründungsakt selbst, sondern umfasst als Dauergewährleistung auch den Bestand und die Betätigung der gegründeten Vereinigung. Zum sachlichen Schutzbereich gehört namentlich das Recht der Mitglieder, die Vereinigung aufrechtzuerhalten, an ihrer internen Willensbildung mitzuwirken und die satzungsmäßigen Zwecke nach außen zu verfolgen. Als „konstituierendes Prinzip der demokratischen und rechtsstaatlichen Ordnung des Grundgesetzes: das Prinzip freier, sozialer Gruppenbildung“

> BVerfGE 50, 290 (353); 149, 160 (192); vgl. auch BVerfGE 146, 164 (194))
> unabhängig vom Staat ((vgl. BVerfGE 146, 164 [193 f. Rn. 78]),

steht die Vereinigungsfreiheit den Kommunikationsgrundrechten nahe. Sachlich schützt Art. 9 Abs. 1 GG nicht nur die bloße Gründung und den Bestand des Vereins, sondern auch seine **vereinsmäßige Betätigung und Funktionsfähigkeit**. Geschützt ist insbesondere die **Verfolgung des satzungsmäßigen Vereinszwecks**. Dazu gehört der Betrieb einer Beratungsstelle sowie die Durchführung vielfältiger Hilfsangebote in den Vereinsräumen.

Vorliegend besteht der Vereinszweck in der **Unterstützung und Beratung von** Sexarbeiter:innen **in ihren Lebenslagen**. Die regelmäßige Inanspruchnahme dieser Angebote durch die Zielgruppe ist für die Erfüllung des Vereinszwecks notwendig. Damit fällt sowohl der **Betrieb der Beratungsstelle** als auch die **ungehinderte Inanspruchnahme durch die Betroffenen** in den sachlichen Schutzbereich des Art. 9 I GG.
Denn geschützt ist auch die tatsächliche Möglichkeit des Vereins, seinen Zweck wirksam zu verwirklichen.

Die Überwachung, gerade mittels biometrischer Echtzeitidentifizierung, berührt den Schutzbereich, da diese eine vollständige und automatisierte Überwachung ermöglicht, wer die Vereinsräume betritt oder verlässt, sich also ggf. beraten lässt. Die Kameraüberwachung entfaltet eine abschreckende Wirkung, da sowohl das Klientel als auch der Anlass der Beratung besonders sensibel sind. Sexarbeitende sind gesellschaftlich einer Stigmatisierung und vielfach auch staatlichen Maßnahmen ausgesetzt.

> Vgl. *Demir*, Zwischen Schutz, Stigma und Stereotyp, https://verfassungsblog.de/zwischen-schutz-stigma-und-stereotyp/ - abgerufen am 21.04.2026.

2. Hoheitlicher Eingriff

Die automatisierte Auswertung der biometrischen Daten der Kläger:innen im Rahmen der biometrischen Echtzeit-Fernidentifizierung nach § 14 Abs. 9 – 11 HSOG stellt einen Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung dar.

Das Recht auf informationelle Selbstbestimmung schützt vor jeder Form der Erhebung, schlichter Kenntnisnahme, Speicherung, Verwendung, Weitergabe oder Veröffentlichung von persönlichen Informationen. Es geht dabei über den durch die Kriterien der Unmittelbarkeit und Finalität geprägten klassischen Eingriffsbegriff hinaus,

> BVerfGE 65, 1 (43); *Di Fabio*, in: Dürig/Herzog/Scholz, Grundgesetz, 106. EL Oktober 2024, Art. 2 Abs. 1 Rn. 176; *Eichberger*, in: Huber/Voßkuhle, Grundgesetz, 8. Auflage 2024, Art. 2 Rn. 289.

Bei der biometrischen Echtzeit-Fernidentifizierung werden fortlaufend biometrische Daten der Gesichtszüge aller ins Blickfeld der Kamera geratenen Personen erfasst und identifiziert,

> vgl. DSFA, Anlage B7, S. 12 f.

Das System erhebt dabei numerische Darstellungen der Gesichter (sog. „Face Embeddings“). Dabei handelt es sich um Vektoren, die Gesichtsmerkmale repräsentieren,

> *Hahn*, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 50.

Dazu wird das Referenzbild in das VAS Videmo360 importiert (DSFA, Anlage B7, S. 7). Im Anschluss werden die so gewonnen Daten mit einem Referenzdatensatz (sog. „Template“) abgeglichen. Dieses Template beinhaltet (eindeutige charakteristische Merkmale der erfassten biometrischen Gesichtsmuster) die Bilder der bestimmten gesuchten Personen. Das System berechnet dabei einen Vergleichswert zwischen den Vektoren in beiden Datensätzen. Ausgerichtet an einem von den zuständigen Polizeibeamt:innen selbst voreingestellten Schwellenwert, der bestimmt, wie ähnlich sich die Vektoren sein müssen, erkennt das System ab einer gewissen Ähnlichkeit einen „Treffer“,

> vgl. DSFA,Anlage B7, S. 8), ferner *Töpfer/Kleemann*, Polizeiliche Gesichtserkennung: Menschenrechtliche Herausforderungen einer Risikotechnologie, 2025, S. 14; Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 50.

Bei der biometrischen Echtzeit-Fernidentifizierung werden folglich biometrische Merkmale des Gesichts erfasst, kurzfristig gespeichert, in ein Template umgewandelt, in einer Referenz-Datenbank gespeichert, anschließend abgeglichen und auf diese Weise verarbeitet,

> vgl. DSFA, Anlage B7, S. 12 f.

Somit wird bei Durchführung der Maßnahme nach 14 Abs. 9 – 11 HSOG durch die automatisierte Erfassung, Speicherung und den Abgleich der biometrischen Daten der Kläger:innen, während sie sich im Sichtfeld der Kamera aufhalten, in ihr Grundrecht auf informationelle Selbstbestimmung eingegriffen.

Einer Einstufung als Eingriff würde es auch nicht entgegenstehen, wenn die Daten unmittelbar wieder gelöscht werden, sollte kein Treffer mit der Datenbank vorliegen. Zum einen sieht die Ermächtigungsgrundlage eine entsprechende Löschpflicht nicht ausdrücklich vor. Aber auch wenn dies ausweislich der Klageerwiderung in der Praxis so gehandhabt wird (Klageerwiderung vom 17. Dezember 2025, S. 9), hat das Bundesverfassungsgericht in seiner Entscheidung zu automatisierten Kfz-Kennzeichenkontrollen explizit festgestellt, dass ein Eingriff auch vorliege, wenn die erfassten Daten im Falle eines Nichttreffers sofort wieder gelöscht würden und dadurch den Betroffenen weder Unannehmlichkeiten noch Konsequenzen erwüchsen. Es führt aus, dass diese Umstände nichts daran ändern,

> *„dass sie durch die Kennzeichenkontrolle einer staatlichen Maßnahme unterzogen werden, mit der sich ihnen gegenüber ein spezifisches Fahndungsinteresse zur Geltung bringt. Mit ihr werden die Betroffenen daraufhin überprüft, ob sie oder die von ihnen mitgeführten Sachen behördlich gesucht werden. Zugleich wird ihre ungehinderte Weiterfahrt unter den Vorbehalt gestellt, dass Erkenntnisse gegen sie nicht vorliegen. Eine solche Maßnahme ist nicht erst hinsichtlich ihrer Folgen, sondern als solche freiheitsbeeinträchtigend. Zur Freiheitlichkeit des Gemeinwesens gehört es, dass sich die Bürgerinnen und Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein* […]*. Jederzeit an jeder Stelle unbemerkt registriert und darauf überprüft werden zu können, ob man auf irgendeiner Fahndungsliste steht oder sonst in einem Datenbestand erfasst ist, wäre damit unvereinbar. Vielmehr bedürfen solche Maßnahmen vor der Freiheit des Einzelnen eines spezifischen Grundes und sind als Eingriffe in das Grundrecht auf informationelle Selbstbestimmung rechtfertigungsbedürftig“,*
>
> BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15, NJW 2019, 827 (830 Rn. 51).

Bei der biometrischen Echtzeit-Fernidentifizierung nach § 14 Abs. 9 – 11 HSOG verdichtet sich das behördliche Fahndungsinteresse an den erfassten Daten in gleicher Weise, da die Maßnahme gerade auf den Abgleich sämtlicher Personen im Sichtfeld gerichtet ist und diese nicht lediglich zufällig am Rande miterfasst werden.

Somit liegt im vorliegenden Fall ein doppelter Eingriff in das Recht auf informationelle Selbstbestimmung vor. Zum einen ist die Erfassung der biometrischen Daten der Kläger:innen und die Generierung der daraus erzeugten Gesichtstemplates als Eingriff einzustufen. Der anschließende Abgleich dieser Daten mit den Gesichtszügen der jeweils gesuchten Person stellt einen weiteren, eigenständigen Eingriff dar,

> vgl. BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15, NJW 2019, 827 (829 Rn. 44 ff.) in Bezug auf die automatisierte KFZ-Kennzeichenkontrolle.

Soweit die mit den biometrischen Daten der Kläger:innen erstellten Gesichtstemplates den von den zuständigen Polizeibeamt:innen jeweils selbst festzulegenden Minderähnlichkeitsschwellenwert überschreiten und damit als Treffer eingeordnet werden, kommt es zu zusätzlichen Eingriffen in ihr Grundrecht auf informationelle Selbstbestimmung durch die Anzeige und Speicherung dieser Treffermeldung, die finale Bewertung dieser durch die polizeilichen Sachbeamt:innen sowie die Hintergrundprotokollierung von Zugriffen auf das VAS Videmo360,

vgl. DSFA, Anlage B7, S. 59.

Darüber hinaus liegt ein Eingriff in das Grundrecht auf Vereinigungsfreiheit aus Art. 9 Abs. 1 GG der Kläger:innen vor. Ein Eingriff liegt in jedem staatlichen Verhalten, das die Ausübung der Vereinigungsfreiheit erschwert oder unmöglich macht.

Die Kameraüberwachung des Bürgersteigs vor dem Vereinsheim kann Personen, die die Beratungsstelle aufsuchen wollen, davon abschrecken, diese tatsächlich zu betreten. Gerade bei einer besonders sensiblen Zielgruppe wie Sexarbeiter:innen besteht ein erhebliches Interesse an Anonymität und Vertraulichkeit. Es ist naheliegend, dass Betroffene aus Furcht vor Identifizierbarkeit oder behördlicher Erfassung von einem Besuch der Beratungsstelle Abstand nehmen. Dadurch wird die Inanspruchnahme der Vereinsangebote erheblich erschwert.

In der Folge kann der Verein seinen satzungsmäßigen Zweck – die Unterstützung von Sexarbeiter:innen in diesen Räumlichkeiten nicht oder nur eingeschränkt erfüllen. Die Maßnahme beeinträchtigt damit die vereinsmäßige Betätigung und Funktionsfähigkeit des Vereins.

Folglich liegt ein mittelbarer faktischer Eingriff in den Schutzbereich des Art. 9 Abs. 1 GG vor

3. Rechtswidrigkeit des Eingriffs

Dieser Eingriff ist rechtswidrig, da die ihm zugrundeliegende Ermächtigungsgrundlage verfassungswidrig ist (dazu unter a), er im Einzelfall unverhältnismäßig ist (dazu unter b) und gegen das Unionsrecht verstößt (dazu unter c).

a) Verfassungswidrigkeit der Ermächtigungsgrundlage

Die auf § 14 Abs. 9 – 11 HSOG gestützten Eingriffe sind verfassungsrechtlich nicht zu rechtfertigen und verletzen die Kläger:innen in ihrem Grundrecht auf informationelle Selbstbestimmung. Es handelt sich um Eingriffe mit einer besonders hohen Intensität (dazu unter aa), für dessen Rechtfertigung es eine hinreichend bestimmte Ermächtigungsgrundlage bedarf (dazu unter bb)), die strenge Vorgaben für die Wahrung der Verhältnismäßigkeit (dazu unter cc)) und angemessene Verfahrensvorschriften (dazu unter dd)) vorsehen muss. Diesen Anforderungen wird § 14 Abs. 9 – 11 HSOG nicht gerecht.

aa) Besonders hohe Eingriffsintensität

Entgegen der Auffassung der Beklagten (Klageerwiderung vom 17. Dezember 2025, S. 7 f.) hat die automatisierte Verarbeitung von biometrischen Daten im Rahmen einer Maßnahme nach § 14 Abs. 9 – 11 HSOG nicht lediglich eine mittlere, sondern eine besonders hohe Eingriffsintensität. Nach der verfassungsrechtlichen Rechtsprechung wird das Gewicht eines Eingriffs vor allem durch das Gewicht des vom Eingriff betroffenen Rechtsguts sowie durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt,

> BVerfGE 65, 1 (45f); BVerfG, Beschluss vom 27.05.2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 129; BVerfG, Beschluss vom 10.11.2020 - 1 BvR 3214/15 -, BVerfGE 156, 11 (48).

Darüber hinaus ist bedeutsam, wie hoch die Sensibilität der erhobenen Daten zu bewerten ist, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben,

> vgl. etwa BVerfG, Urteil vom 2.03.2010 - 1 BvR 256/08 -, - 1 BvR 263/08 -, -1 BvR 586/08 -, BVerfGE 125, 260 (310 f., 318 ff., 320).

Auch die Heimlichkeit einer staatlichen Eingriffsmaßnahme erhöht deren Eingriffsgewicht,

> BVerfG, Beschluss vom 24.11.2024 - 1BvL 3/22 -, juris Rn 93; BVerfG, Beschluss vom 27.05.2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, juris Rn. 129.

Schließlich kann je nach Einsatzart die Verwendung lernfähiger Systeme, also Künstlicher Intelligenz besonderes Eingriffsgewicht haben,

> BVerfG, Urteil vom 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1205 Rn. 100).

(1) Verwendung biometrischer Daten

Zunächst folgt bereits aus der Art der verwendeten Daten eine hohe Eingriffsintensität. Entgegen der Auffassung der Beklagten (Klageerwiderung vom 17. Dezember 2025, S. 8) wird nicht lediglich der Standort einer konkreten gesuchten Person erhoben, sondern die biometrischen Daten aller Personen, die sich im Kamerasichtfeld befinden verarbeitet. Auch wenn ausweislich der Klageerwiderung und Datenfolgenabschätzung derzeit im Rahmen des einjährigen Pilotprojekts nur biometrische Gesichtsdaten verarbeitet werden (Klageerwiderung vom 17. Dezember 2025, S. 6 und , DSFA, Anlage B7, S. 7), lässt der weite Wortlaut grundsätzlich auch die Erfassung, Speicherung und den Abgleich anderer biometrischer Merkmale wie Gang- oder Spracherkennung zu. Ebenso benennt die Datenschutzfolgeabschätzung explizit das polizeiliche Bedürfnis KI-gestützte digitale Fernidentifizierungssysteme einzusetzen, die sowohl Gesichter als auch Körpermuster anhand biometrischer Muster erkennen,

> vgl. DSFA, Anlage B7, S. 4.

Vor diesem Hintergrund ist nicht auszuschließen, dass zukünftig die Maßnahmen nach § 14 Abs. 9 – 11 HSOG auch auf die Erfassung und den Abgleich anderer biometrischer Daten ausgeweitet wird.

Biometrische Daten – insbesondere in Bezug auf das Gesicht – sind auf besondere Weise persönlichkeitsrelevant und gehen in ihrer Sensibilität weit über reine Standortdaten hinaus. Sie können ohne körperliche Verletzungen weder verändert noch abgelegt werden. Per-

sonen, die für die Maßnahme keinen Anlass gegeben haben, können sich dieser auch kaum entziehen, ohne ihr Verhalten derart anzupassen, dass sie die betreffenden Orte gänzlich meiden.

Auch das BVerfG ordnet das Gesicht insofern als „höchstpersönliches Merkmal“ ein,

> BVerfG, Beschluss vom 18.12.2018 - 1 BvR 142/15 -, NJW 2019, 827 (830 Rn. 53).

Die Eingriffsintensität lässt sich nach der Faustregel „Je persönlicher das Merkmal, desto intensiver der Eingriff“ damit als deutlich gesteigert bewerten,

> *Kulick*, „Höchstpersönliches Merkmal“ – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, NVwZ 2020, 1622 (1625).

Die Erhebung und Verwertung biometrischer Daten haben zudem eine besondere grundrechtliche Relevanz über den Schutz der Freiheitsrechte des Einzelnen hinaus. Das BVerfG fasst diese Dimension wie folgt zusammen:

> *„Zur Freiheitlichkeit des Gemeinwesens gehört es, dass sich die Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein“,*
>
> BVerfG, Beschluss vom 18.12.2018 - 1 BvR 142/15 -, NJW 2019, 827 (830 Rn. 51).

Die Auffassung der Beklagten, dass die Eingriffsintensität dadurch verringert sei, dass keine vertraulichen Verhaltensweisen erfasst würden, sondern lediglich das Bewegungsverhalten im öffentlichen Raum, das ohne weiteres auch für alle Personen, die sich dort aufhalten, erkennbar sei (Klageerwiderung vom 17. Dezember 2025, S. 9), ist unzutreffend. Denn die Echtzeit-Fernidentifizierung geht weit über eine normale Videoüberwachung hinaus, indem sie nicht nur das Bewegungsverhalten, sondern biometrische Gesichtsdaten automatisiert erfasst, speichert und abgleicht. Die Umwandlung der Gesichtszüge in numerische Vektoren und die damit einhergehende Möglichkeit der eindeutigen Identifizierung von Personen ist

gerade nicht ohne weiteres für Menschen, die sich sonst an dem von der Kamera erfassten Ort aufhalten, erkennbar.

(2) Heimlichkeit der Maßnahme

Auch die Heimlichkeit einer staatlichen Eingriffsmaßnahme führt zur Erhöhung ihrer Intensität,

> BVerfG, Beschluss vom 27.05.2020 - 1 BvR 1873/13 und 1 BvR 2618/12 -, Rn. 129; BVerfGE 156, 11 (48).

Grund dafür ist, dass mit der Heimlichkeit eine faktische Verwehrung vorherigen Rechtsschutzes und die Erschwerung nachträglichen Rechtsschutzes einhergeht, sofern dieser überhaupt zu erlangen ist,

> BVerfG, Urteil vom 27.05.2005 - 1 BvR 668/04 -, BVerfGE 113, 348 (383); BVerfG, Beschluss vom 13.06.2007 - 1 BvR 1550/03 -, BVerfGE 118, 168 (197); BVerfGE 156, 11 (48).

Die Videoüberwachung nach § 14 Abs. 1, 3, 3a und 4 HSOG, die die Maßnahmen nach § 14 Abs. 9 HSOG ermöglicht, erfolgt zwar offen. Die tatsächlich durchgeführte Echtzeit-Fernidentifizierung erfolgt jedoch heimlich. Der Eingriff wird entgegen der Annahme in der Datenschutzfolgenabschätzung (DSFA, Anlage B7, S. 10. 65) auch nicht dadurch offen gelegt, dass gemäß § 14 Abs. 3 i.V.m. Abs. 10 S. 4 HSOG die Video-Aufnahmebereiche mit Hinweis auf eine mögliche Echtzeit-Fernidentifizierung ausgeschildert werden. Es ist Betroffenen nicht möglich zu erkennen, welche Kameras die Funktion eingeschaltet haben, wann, wie lange oder wie oft dies geschieht. Entgegen der Annahme in der Datenschutzfolgenabschätzung (DSFA, Anlage 7, S. 69) führen diese Umstände dazu, dass es sich um eine heimliche Überwachungsmaßnahme handelt. Zudem können etwaige Betroffene können auch im Nachhinein nicht nachvollziehen, ob und wann entsprechende Maßnahmen gegen sie stattgefunden haben, da sie weder während noch nach Beendigung der Maßnahmen benachrichtigt werden. Ein effektiver Rechtsschutz bleibt damit faktisch verwehrt. In einem nachfolgenden Abschnitt räumt die Datenschutzfolgenabschätzung selbst den „verdeckten Cha-

rakter der gezielten Suche“ ein, der zu einer faktischen Beschränkung des Beschwerde- und Rechtswegs führe,

vgl. DSFA, Anlage B7, S. 69.

Nach den Ausführungen in der Datenschutzfolgenabschätzung bestehe „eine Überprüfungsmöglichkeit [...] faktisch nur dann, wenn Treffer-Ergebnisse Anlass zu Folgemaßnahmen geben, die dann zum Gegenstand von Beschwerde-, Widerspruchs-, Gerichts- oder sonstigen Prüfverfahren werden“,

DSFA, Anlage B7, S. 67.

Die Kläger sind in der Regel mindestens an [redacted] Tagen die Woche in den Vereinsräumlichkeiten, sie werden also regelmäßig von den Kameras erfasst. Damit steigt auch die Wahrscheinlichkeit, dass sie auch von einer Auswertung des Videomaterials durch das KI-System betroffen sind. Die Heimlichkeit der Maßnahme verstärkt also in diesem Fall den Eingriff besonders, da die Kläger nicht nachvollziehen können, ob und wann sie von der KI-Auswertung betroffen sind.

(3) Erhebliche Streubreite

Die Eingriffsintensität wird weiter dadurch erhöht, dass die Maßnahme eine erhebliche Streubreite aufweist. Mit diesem Begriff ist das Maß gemeint, in dem Menschen durch eine Maßnahme erfasst werden, die persönlich keinen Anlass zur Verarbeitung ihrer Daten gegeben haben,

BVerfG, Urteil vom 16.02.2023 – 1 BvR 2634/20 -, BVerfGE 165, 363 (400f.).

Wird die Echtzeit-Fernidentifizierung nach § 14 Abs. 9 HSOG eingesetzt, betrifft sie alle Personen im von der Videokamera erfassten, öffentlichen Bereich. Eine weitere Differenzierung findet nicht statt. Betroffen sind sowohl Personen, die sich regelmäßig in dem überwachten Bereich aufhalten, als auch solche, die nur einmal und/oder kurz in das Blickfeld der Kamera geraten.

Das Polizeipräsidium Frankfurt am Main geht in seiner Datenschutz- und Grundrechtefolgenabschätzung selbst davon aus, dass der Einsatz der biometrischen Echtzeit-Fernidentifizierung „einer systematischen Überwachung durch die Verarbeitung von Bildmaterial von Videoschutzanlagen im öffentlichen Raum“ nahe komme und „auch besonders schutzbedürfte Personen betreffen“ könne, etwa „behinderte, gebrechliche und besonders alte Menschen, sprach- und kulturunkundige Ausländer und solche ohne gesicherten Aufenthaltsstatus“,

> DSFA, Anlage B7, S. 56.

Bei dem Bereich, der von der Maßnahme erfasst wird, handelt es sich zudem – auch wenn nicht das gesamte Bahnhofsviertel von Kameras mit der entsprechenden Funktion überwacht wird – um einen überdurchschnittlich hoch frequentierten Ort. Zu den 3.500 Personen, die im Viertel wohnen und den 23.000 Personen, die dort ihren Arbeitsplatz haben, kommen weitere rund 500.000 Personen, die täglich den Bahnhof nutzen,

> vgl. Stadt Frankfurt am Main, Koordinierungsbüro Bahnhofsviertel – Wirtschaft, Handel und Tourismus, abrufbar unter https://frankfurt.de/service-und-rathaus/verwaltung/aemter-und-institutionen/koordinierungsbuero-bahnhofsviertel/handel-versorgung-produktivitaet-und-tourismus (Letzter Abruf: 15.01.2026)

(4) Art und Weise der Durchführung mitttels Künstlicher Intelligenz

Auch die konkrete Art und Weise der Durchführung erhöht die Eingriffsqualität der Maßnahme. Das Recht auf informationelle Selbstbestimmung soll insbesondere davor schützen, dass personenbezogene Daten von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können. Die daraus resultierende Gefahr für die freie Persönlichkeitsentfaltung besteht in besonderem Maße unter den Anwendungsmöglichkeiten elektronischer Datenverarbeitung,

> *Eichberger*, in: Huber/Voßkuhle, Grundgesetz, 8. Auflage 2024, Art. 2, Rn. 287.

Die konkrete technische Umsetzung – die Verwendung von algorithmenbasierter, voll automatisierter künstlicher Intelligenz zum Datenabgleich – birgt spezifische Probleme, die Überschaubarkeit und Beherrschbarkeit der Maßnahme deutlich verringern. Die Algorithmen sind eine „Blackbox“ dergestalt, dass sie Daten auf eine hochkomplexe und/oder komplizierte Weise auswerten – Menschen ist es damit oft unmöglich, diesen Prozess nachzuvollziehen. Wie die Technologie zu dem Ergebnis kommt, welches sie präsentiert, kann dann selbst von den Anwender:innen nicht erklärt werden. Damit ist auch die Verifizierbarkeit der Ergebnisse eingeschränkt,

> *Rademacher/Perkowski*, Staatliche Überwachung, neue Technologien und die Grundrechte, JuS 2020, 713 (716).

Die mangelhafte Nachvollziehbarkeit und Verifizierbarkeit wird teilweise kompensiert, da Polizeibeamt:innen einen positiven Treffer durch einen eigenen Abgleich der zwei konkreten Bilder kontrollieren können. Dies ist aber zum einen nicht gesetzlich vorgegeben. Darüber hinaus bleibt für Grundrechtsträger:innen aber auch die begründete Sorge, dass ein Abgleich durch eine nicht nachvollziehbare Methodik durchgeführt wird. So bleibt ein Schutz etwa vor diskriminierend wirkenden Systemfehlern, die zu falsch positiven Ergebnissen führen können, verwehrt.

Auch das Bundesverfassungsgericht hat anerkannt, dass einer automatisierten Datenanalyse oder -auswertung potenziell ein Eigengewicht zukommt, das zu weitergehenden Rechtfertigungsanforderungen führt,

> BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19 und 1 BvR 2634/20 -, NJW 2023, 1196 (1199 Rn. 54).

Während allgemein der Grundsatz der Verhältnismäßigkeit die Weiterverarbeitung bereits erhobener Daten verhältnismäßig macht, ist das bei einer automatisierten Datenanalyse und -verarbeitung mitunter nicht ausreichend. Grund dafür ist, dass die Automatisierung die Verarbeitung großer und komplexer Informationsbestände ermöglicht, die die tatsächlichen Kapazitätsgrenzen herkömmlicher polizeilicher Arbeit weit übersteigt,

> BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19 und 1 BvR 2634/20 -, NJW 2023, 1196 (1201 Rn. 69f).

Das spezifische Eigengewicht einer automatisierten Datenanalyse ist nach verfassungsgerichtlicher Rechtsprechung dabei nicht immer gleich, sondern hängt von der näheren Ausgestaltung der Befugnis ab. Ausschlaggebend ist, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden,

> BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19 und 1 BvR 2634/20 -, NJW 2023, 1196 (1201 Rn. 66, 76).

Die Weiterverarbeitung entfaltet im vorliegenden Fall ein spezifisches Eigengewicht, das nicht allein über den Grundsatz der Zweckbindung gerechtfertigt werden kann. Zwar sieht § 14 Abs. 9 - 11 HSOG vor, dass lediglich in einem begrenzten Zeitraum an einem begrenzten Ort erhobene Daten in einfacher Form abgeglichen werden. Allerdings handelt es sich um höchstpersönliche Daten (s.o. II.1.c.aa.(1)(a)), die zudem potenziell von vielen tausend Menschen ohne deren Wissen erfasst werden.

(5) Gefahren technischer Ausführung

Die technische Umsetzung des § 14 Abs. 9 HSOG – also die Nutzung von Gesichtserkennungsalgorithmen zu Identifizierungszwecken – geht mit unterschiedlichen Gefahren einher, die die Eingriffsintensität weiter erhöhen.

Zunächst ist die Zuverlässigkeit der Gesichtserkennung fehleranfällig, was die Eingriffsintensität einer automatisierten Datenanalyse erhöhen kann,

> vgl. BVerfGE 165, 363 (409).

Aktuelle Tests des US-amerikanischen National Institute of Standards and Technology (NIST) ergeben, dass selbst unter optimalen Bedingungen – dem Abgleich einer Datenbank von 12 Millionen Datensätzen mit frontal aufgenommenen aufgenommen Porträtfotos guter

Qualität – die Fehlerquote („false negative rate“) der Gesichtserkennung bei 0,1 Prozent lag. Das bedeutet bereits einen Fehler auf 1.000 Personen, eine Zahl von Menschen, die an einem belebten Ort wie einem Bahnhof, ohne weiteres in kurzer Zeit erreicht wird. Haben die Aufnahmen, die für den Abgleich mit der Datenbank verwendet werden, eine schlechtere Qualität – wie es bei Überwachungsmaßnahmen mit Hilfe von Kameras der Fall ist – liegt die Quote der Erkennungsfehler (je nach Algorithmus) bei bis zu 20 Prozent. Diese Rate lässt sich technisch nur zu der Bedingung senken, dass der Algorithmus mehr „false positives“ ausgibt.

> *Grother/Ngan/Hanaoka*, Face recognition technology evaluation (FRTE). Part 2: Identification, 2025, abrufbar unter https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (Letzter Abruf: 31.12.2025).

Diese Fehleranfälligkeit kann dazu führen, dass es einerseits zu „falsch positiven“ Treffern kommt. Dadurch können gänzlich Unbeteiligte, die für die Maßnahme keinen Anlass gegeben haben, fälschlicherweise als die gesuchte Person identifiziert und so Adressat weiterer (teils eingriffsintensiver und weitgehender) gefahrenabwehrrechtlicher Folgemaßnahmen werden.

Dieses Risiko wird insbesondere dadurch verstärkt, dass ausweislich der Klageerwiderung sowie der Datenschutz- und Grundrechtefolgenabschätzung (Klageerwiderung vom 17. Dezember 2025, S. 9, Anlage B7, S. 8 f.) die zuständigen Polizeibeamt*innen bei jedem Einsatz der biometrischen Echtzeit-Fernidentifizierung selbst eine nach Prozentpunkten skalierte Mindestähnlichkeitsschwelle bestimmen, „anhand derer das VAS Videmo360 die Templates mit dem Referenzmaterial automatisiert abgleicht und dem Nutzer die erkannten Übereinstimmungen über der Mindestähnlichkeitsschwelle („Treffermeldung“) anzeigt“. Die manuelle Einstellung der Ähnlichkeitsschwelle bestimme die Anzahl der systembedingten Treffermeldungen. Alle Treffermeldungen mit dem vom VAS erkannten Bild der erfassten Personen werden gespeichert. Treffermeldungen zu einer (bekannten oder unbekannten) Person können vor einem erneuten Abgleich optional zu einer „Identität“ zusammengefasst werden, um die Genauigkeit der Übereinstimmungssuche zu erhöhen,

> vgl. DSFA, Anlage B7, S. 8f.

Je niedriger diese Schwelle angesetzt wird, desto mehr Personen können als Treffer erfasst werden. Mit steigender Trefferzahl erhöht sich zugleich die Anzahl der Betroffenen, bei denen der Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung durch die längerfristige Speicherung ihrer biometrischen Daten vertieft wird, als auch die Wahrscheinlichkeit von Fehlidentifikationen und ungerechtfertigten polizeiliche Anschlussmaßnahmen. Auch die Zusammenfassungen von Treffermeldungen zu einer „Identität“ sind fehleranfällig und steigern das Risiko, dass Unbeteiligte zum Gegenstand weiterer polizeilicher Maßnahmen werden. Da die Rechtsgrundlage weder Vorgaben noch Begrenzungen für die Festlegung einer verbindlichen Mindestähnlichkeitsschwelle enthält und die damit einhergehende Festlegung der Reichweite und Trefferanzahl dem freien Ermessen der handelnden Behörde überlassen wird, erhöht sich das Eingriffsgewicht erheblich.

Darüber hinaus besteht die Gefahr von „falsch negativen“ Ergebnissen, bei denen der Algorithmus die gesuchte Person trotz Abgleich fehlerhaft nicht erkennt. Das kann dazu führen, dass die Maßnahme nach § 14 Abs. 9 HSOG weiter oder länger ausgeweitet wird, als tatsächlich nötig und so mehr Personen Betroffene der Maßnahme sind.

Dieser Aspekt wurde bei der Risikobewertung im Rahmen der Datenschutzfolgenabschätzung jedoch nicht berücksichtigt. Zwar werden dort Qualitätsmängel der Referenzbilder ausdrücklich als beträchtliche Fehlerquelle anerkannt und eingeräumt, dass fehlerhafte Suchergebnisse sich insbesondere „bei ungünstigen Licht- und Witterungsverhältnissen oder einer großen Anzahl der den Aufnahmebereich der VSA durchlaufenden Personen einstellen" können,

vgl. DSFA, Anlage B7, S. 91 ff.

Die damit verbundene Schlussfolgerung, dass falsch negative Ergebnisse zu einer zeitlichen oder räumlichen Ausweitung der Maßnahme und damit zu einer Vertiefung des Eingriffs für unbeteiligte Dritte führen können, zieht die Datenschutzfolgenabschätzung jedoch nicht.

Die automatisierte Verarbeitung von Bild- und Videodateien birgt zudem erhebliche Diskriminierungsrisiken. Es besteht ein hohes Risiko algorithmischer Verzerrungen und Fehlidentifikationen,

Haley, The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent, 2025, abrufbar unter https://www.mdpi.com/1424-8220/25/10/3160 (Letzter Abruf: 31.12.2025).

Grund dafür ist, dass die Künstliche Intelligenz, welche die Gesichtserkennung ausführt, teils auf verzerrten Trainingsdatensätzen beruht. Infolgedessen ist die Fehlerquote nicht gleichmäßig über alle Bevölkerungsgruppen verteilt. Das konnte ein Test der NIST 2019 belegen, der 189 Algorithmen umfasste. Das Institut stellte fest, dass sowohl die Erkennung von Persons of Colour, als auch von Frauen, Kindern und älteren Menschen deutlich fehleranfälliger ist als weißen Männern mittleren Alters,

Grother/Ngan/Hanaoka, Face recognition vendor test (FRVT). Part 3: Demographic effects, 2019, abrufbar unter https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (Letzter Abruf: 31.12.2025); siehe auch *Limanté*, Bias in facial recognition technologies used by law enforcement. Understanding the causes and searching for a way out, Nordic Journal of Human Rights 42 (2), 2024, S. 115–134.

Dieser Aspekt findet in der Risikobewertung im Rahmen der Datenschutz- und Grundrechtefolgenabschätzung, nach der ein Diskriminierungsrisiko nicht erkennbar sei (vgl. DSFA, Anlage B7, S. 95 f., 110), keinerlei Berücksichtigung. Auch gesteht das Polizeipräsidium Frankfurt am Main in seiner Datenschutzfolgenabschätzung ein, dass die „Erzeugung der Gesichtstemplates [...] durch ein KI-Modell [erfolgt], dessen genaue Spezifikationen nur dem Hersteller des VAS bekannt ist“ - aber nicht der das System nutzenden Polizeibehörde,

vgl. DSFA, Anlage B7, S. 12.

Es besteht mithin die Gefahr, dass Angehörige dieser Personengruppen bei der Echtzeit-Fernidentifizierung häufiger falsch positiv erkannt werden und infolgedessen weiterreichenden Gefahrenabwehrmaßnahmen ausgesetzt sind. Damit gehen Gefahren für die Handlungsfreiheit Einzelner sowie Verletzungen des Diskriminierungsverbot gem. Art. 3 GG einher. Vor diesem Hintergrund ist die Bewertung in der Datenschutzfolgenabschätzung nicht haltbar, dass alle unbeteiligte Personen beim Einsatz des KI-Systems „anonym bleiben“ und insoweit „keinerlei weitere Belastungen sich an die Erfassung anschließen“,

DSFA, Anlage B7, S. 70.

Diese Einschätzung blendet aus, dass eine niedrig angesetzte Mindestähnlichkeitsschwelle und das überproportionale Fehlerrisiko bei bestimmten Personengruppen dazu führen, dass eine nicht unerhebliche Zahl von Personen, die nicht die jeweils gesuchte Person darstellen, gleichwohl dem Risiko polizeilicher Anschlussmaßnahmen ausgeliefert ist.

(6) Möglichkeit der Verknüpfung von Informationen

Die grundsätzliche Möglichkeit, Informationen zusammenzuführen und Bewegungs- oder Persönlichkeitsprofile von Personen zu erstellen, erhöht die Eingriffsintensität, auch ohne dass tatsächlich derartige Profile erstellt werden. Auf die bloße Möglichkeit der Verknüpfung stellt auch das Bundesverfassungsgericht ab, dass es als eingriffsintensivierend ansieht, wenn durch eine Technik „umfassende Bewegungsprofile erstellt werden könnten“,

> BVerfGE 125, 260 (292); vgl. auch *Hahn*, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 118 m.w.N.

Grund dafür ist, dass das Recht auf informationelle Selbstbestimmung auch dazu dient, Gefährdungen im Vorfeld der Bedrohung konkreter Rechtsgüter zu verhindern,

> BVerfG, Beschluss vom 18.12.2018 - 1 BvR 142/15 -, BVerfGE 150, 244 (264).

Auch das Missbrauchspotential, das mit einer Datensammlung einhergeht, erhöht dementsprechend die Intensität des Eingriffs,

> BVerfGE 125, 260 (320).

Die Erhebung biometrischer Gesichtsdaten macht es leicht, (Bewegungs-)Profile von Personen zu erstellen, da beispielsweise Video- und Fotoaufnahmen, die bereits in staatlichen Datenbanken vorhanden sind, zusammengeführt werden könnten,

> Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 119.

Die Rechtsgrundlage enthält außer für Fälle des § 14 Abs. 11 S. 5 HSOG keine Löschpflichten für erhobene Daten. Rein technisch wäre es daher möglich, bei wiederholtem Einsatz der Echtzeit-Fernidentifizierung Muster zu erkennen, wer sich wann und wie regelmäßig an den überwachten Orten aufhält.

Der Beklagte verkennt insoweit, dass diese Verknüpfungsgefahr nicht durch eine räumliche Beschränkung auf den jeweiligen Kamerabereich entschärft und dadurch die Eingriffsintensität nicht entscheidend relativiert wird (vgl. Klageerwiderung vom 17. Dezember 2025, S. 9). Auch innerhalb eines begrenzten Aufnahmebereichs können Verhaltensmuster, Routinen sowie Rückschlüsse auf persönliche Neigungen oder Vorlieben erfasst und ausgewertet werden.

Dem steht auch die Einschätzung in der Datenschutzfolgenabschätzung nicht entgegen, wonach die gezielte Suche lediglich eine punktuelle Momentaufnahme des Aufenthalts einer Person darstelle,

> vgl. DSFA, Anlage B7, S. 69.

Das Bundesverfassungsgericht hat klargestellt, dass für eine Erhöhung des Eingriffsgewichts gerade nicht erforderlich ist, dass ein lückenloses Bewegungs- und Verhaltensbild erfasst werden kann. Auch lückenhafte Bewegungsprofile können einen schwerwiegenden Eingriff mit hoher Persönlichkeitsrelevanz darstellen. Es führt dazu aus, dass

> *„Eingriffsgewicht* […] *allerdings bereits dann nicht unerheblich erhöht* [wird], ***wenn punktuelle Maßnahmen über einen längeren Zeitraum hinweg durchgeführt werden****. Denn so kann unter Umständen nach und nach doch ein Bewegungsprofil oder Bewegungsbild der Person mit erhöhter Persönlichkeitsrelevanz zusammengestellt werden (vgl. BVerfGE 120, 378 Rn. 416 f. = NJW 2008, 1505; BVerfGE 165, 1 Rn. 175 = NVwZ-Beil 2023, 37). Umgekehrt können auch* ***in sehr enger zeitlicher Taktung erfolgende Standortermittlungen****, die über einen* ***kürzeren Zeitraum erfolgen****, das* ***Eingriffsgewicht einer Maßnahme erhöhen****. Denn sie ermöglichen die Erstellung eines detaillierten und für einen begrenzten Zeitraum nahezu vollständigen Bewegungsprofils, das unter Umständen sehr genau über den gewöhnlichen Tagesablauf einer Person Auskunft geben und insoweit eine potenziell hohe Persönlich-*

> *keitsrelevanz haben kann. Einen schwerwiegenden Eingriff begründen jedenfalls Maßnahmen, mit denen der Standort einer Person sowohl im engen Zeittakt als auch über einen längeren Zeitraum hinweg ermittelt werden kann (vgl. BVerfGE 162, 1 Rn. 321 = NVwZ-Beil 2022, 70). Dabei können* ***grundsätzlich auch lückenhafte Bewegungsprofile*** *einen schwerwiegenden Eingriff mit hoher Persönlichkeitsrelevanz darstellen. Denn auch durch sie können Verhaltensweisen, Routinen, persönliche Neigungen und Vorlieben relativ zuverlässig überwacht werden"* [Hervorhebungen durch Unterzeichner],
>
> BVerfG Beschluss vom 17. Juli 2024 – 1 BvR 2133/22, NVwZ-RR 2025, 10, (16 Rn. 130).

Das Bestehen dieses Risikos wird auch durch die eigenen Angaben des Polizeipräsidiums Frankfurt am Main in der Datenschutzfolgenabschätzung untermauert. Dort wird ausgeführt, dass die durch das KI-System erzeugten Daten auch für „die Nachverfolgung der gesuchten Person im Anschluss an Treffermeldungs-Fälle und Veranlassung lageangepasster Folgemaßnahmen" genutzt würden,

> vgl. DSFA, Anlage B7, S. 17.

Die dortige Einordnung, ein solcher Einsatz sei „nicht mehr Teil der eigentlichen gezielten Suche mittels der biometrischen Echtzeit-Fernidentifizierung, sondern deren Folge" (DSFA, Anlage B7, S. 17), ändert nichts an der dadurch erhöhten Eingriffsintensität, da dies auch im Rahmen der auf § 14 Abs. 9 – 11 HSOG gestützten Maßnahmen erfolgen soll.

Ebenfalls nicht zu überzeugen vermag die Annahme in der Datenschutzfolgenabschätzung, die Betroffenen würden den Aufnahmebereich „mehr oder weniger zügig durchqueren", sodass der Erkenntnisgewinn der gezielten Suche auf den Aufenthalt dieser Person als Momentaufnahme beschränkt bleibe,

> vgl. DSFA, Anlage B7, S. 69.

Zum einen erfasst die Maßnahme auch Personen, die sich nicht lediglich durch den Kamerabereich bewegen, sondern einen bestimmten Ort im Sichtfeld der Kamera gezielt aufsuchen – sei es aus beruflichen oder privaten Gründen. Das gilt im vorliegenden Fall in besonderem

Maße. Eine der Kameras erfasst den Eingangsbereich der Beratungsstelle des Vereins Doña Carmen e.V. Personen, die diese Beratungsstelle aufsuchen, bewegen sich nicht flüchtig durch den Kamerabereich, sondern halten sich gezielt dort auf. Das erlaubt Rückschlüsse auf sensible persönliche Umstände, die weit über eine bloße Momentaufnahme hinausgehen.

Zum anderen richtet sich der örtliche Umfang der erfassten Bewegungen nach der Anzahl der eingesetzten Kamerasysteme. Werden – wie im vorliegenden Fall – mehrere Kameras an verschiedenen Standorten betrieben, erstreckt sich die Erfassung über einen erheblichen räumlichen Bereich und ermöglicht die Rekonstruktion von Bewegungsmustern, die weit über das Sichtfeld einer einzelnen Kamera hinausgehen.

Dass diese räumliche Reichweite zukünftig noch erheblich ausgeweitet werden kann, belegt die Ankündigung des Hessischen Ministeriums des Innern, die Maßnahme auch an der Konstablerwache und der Hauptwache einzusetzen,

> Pressemitteilung des Hessischen Ministeriums des Innern, für Sicherheit und Heimatschutz vom 8. April 2026, abrufbar unter https://innen.hessen.de/presse/ki-gestuetzte-videoschutzanlage-in-frankfurt-ausgeweitet (Letzter Abruf: 13. April 2026).

Mit der Ausweitung des Kameranetzes wächst zugleich die Möglichkeit, über mehrere Standorte hinweg detaillierte Bewegungs- und Verhaltensprofile zu erstellen – und damit das Eingriffsgewicht weiter zu erhöhen.

In zeitlicher Hinsicht kommt hinzu, dass die Maßnahme nach den Angaben in der Datenschutzfolgenabschätzung bei jedem Einsatz einen Zeitraum von bis zu drei Monaten umfassen kann, der bei Folgeanträgen um weitere drei Monate verlängert werden kann,

> vgl. DSFA, Anlage B7, S. 67.

Damit erstreckt sich die Maßnahme auf einen erheblichen Zeitraum, der – gemessen an den vom Bundesverfassungsgericht aufgestellten Maßstäben – die Erstellung aussagekräftiger Bewegungsprofile ohne weiteres ermöglichen kann. Dass die gesetzliche Grundlage – an-

ders als bei anderen verdeckten Maßnahmen zur Informationsgewinnung nach §§ 15 ff. HSOG – keine gesetzliche Höchstfrist vorsieht, verstärkt dieses Risiko.

Die Möglichkeit ein Bewegungsmuster zu erstellen, wird auch nicht durch eine vermeintliche technische Ausblendung von Privatzonen (vgl. Klageerwiderung vom 17. Dezember 2025, S. 3), verhindert. Wie der vorliegende Fall eindrücklich zeigt, beschränkt sich die Schwärzung auf vereinzelte Hauseingänge, ohne ein konsistentes oder nachvollziehbares Schutzkonzept erkennen zu lassen. So wird zwar der Hauseingang der Beratungsstelle durch einen schwarzen Balken unkenntlich gemacht, nicht jedoch die Eingänge der angrenzenden Gebäude,

> vgl. Anlage B5.

Für Betroffene ist weder erkennbar, nach welchen Kriterien bestimmte Bereiche als „Privatzonen" eingestuft werden, noch wie die konkrete Auswahlentscheidung getroffen wird. Entscheidend ist zudem, dass Bürgersteig und Straße weiterhin vollständig im Erfassungsbereich der Kamera liegen. Damit bleibt auch bei einem geschwärzten Hauseingang klar erkennbar, welche Personen welche Gebäude betreten und verlassen. Die behauptete eingriffsmildernde Wirkung der Ausblendung geht damit ins Leere.

In Bezug auf die zuständige Polizeibehörde bedeutet dies, dass sie anhand der biometrischen Videoüberwachung im vorliegenden Fallnachvollziehen kann, wann und wer, die Vereinsräume betritt. Dadurch ergibt sich die Möglichkeit,ein Bewegungsmuster zu erstellen, was die Eingriffsintensität bestärkt.

(7) Erzeugung von „Chilling Effects“

Schließlich droht durch die Möglichkeit, an öffentlichen Orten eine KI-basierte Echtzeit-Fernidentifizierung vorzunehmen, dass Abschreckungs- und Einschüchterungseffekte (sogenannte „chilling effects“) entstehen. Damit ist das Phänomen gemeint, dass Menschen ihr Verhalten anpassen, wenn Überwachungsmaßnahmen – auch ohne erkennungsdienstliche Maßnahmen – getroffen werden,

> BVerfG, Urteil vom 11.03.2008 - 1 BvR 2074/05 und 1 BvR 1254/07 -, juris Rn. 78.

Das BVerfG hat die Bedeutung dieser „chilling effects“ für die Wahrnehmung der Grundrechte bereits früh erkannt:

> „*Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden,* ***wird versuchen, nicht durch solche Verhaltensweisen aufzufallen****. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die* ***individuellen Entfaltungschancen des Einzelnen beeinträchtigen****, sondern* ***auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist***“ [Hervorhebungen durch Unterzeichner],
>
> BVerfGE 65, 1 (43).

Die Bedeutung der „chilling effects“ ist in der verfassungsgerichtlichen Rechtsprechung seitdem vielfach weiter besprochen und ausgeformt worden,

> etwa BVerfG, Beschluss vom 5.07.1995 – 1 BvR 2226/94 -, BVerfGE 93, 181 (188ff.); BVerfG, Urteil vom 14.07.1999 – 1 BvR 2226/94 -, - 1 BvR 2420/95 -, - 1 BvR 2437/95 -, BVerfGE 100, 313 (358 f., 381); BVerfG, Urteil vom 12.03.2003 – 1 BvR 330/96 -, - 1 BvR 348/99 -, BVerfGE 107, 299 (310 ff.); BVerfG, Beschluss vom 3.03.2004 – 1 BvF 3/92 -, BVerfGE 110, 33 (53 ff.).

2007 hat das BVerfG bestätigt, dass bereits bei offener Videoüberwachung eines öffentlichen Ortes von einem deutlichen „chilling effect“ auszugehen sei, denn diese

> *„kann und soll zugleich abschreckend wirken und insofern das Verhalten der Betroffenen lenken“,*

BVerfG, Beschluss vom 23.02.2007 - 1 BvR 2368/06 -, NVwZ 2007, 688 (690).

Der vorliegende Fall geht über eine bloße offene Videoüberwachung hinaus. Die erhobenen Daten werden in Echtzeit und voll automatisiert abgeglichen. Die Funktionsweise des Abgleichs ist den Betroffenen dabei nicht bekannt. Es ist deshalb von deutlich stärkeren „chilling effects“ auszugehen, als sie eine Videoüberwachung mit sich ziehen würde.

Außerdem handelt es sich bei der vom Überwachungsraum der Kameras erfassten Eingang der Vereinsräume des Dona Carmen e.V. um einen Ort, an den zum Beispiel auch Sexarbeiter:innen zur Beratungsgesprächen kommen. Die Überwachung durch Kameras und die Nachvollziehbarkeit dessen, wer die Vereinsräume betritt kann auf die Betroffenen eine abschreckende Wirkung haben, da die Wahrnehmung eines persönlichen Beratungsgesprächs durchaus etwas höchst-persönliches und privates sein kann, bei dem man nicht beobachtet werden will.

Wegen der stark verhaltensbeeinflussenden Wirkung verstärkt der chilling effect die Eingriffsintensität,

Vgl. BVerfG, Urteil vom 27.02.2007 - 1 BvR 538/06 -, - 1 BvR 2045/06 -, BVerfGE 117, 244 (259); BVerfG, Beschluss vom 10.12.2012 - 1 BvR 1739/04 -, NJW 2011, 1859 (1860).

(8) Eingriffsmildernde Faktoren ohne wesentliches Gewicht

Die Ermächtigung nach § 14 Abs. 9 – 11 HSOG sieht zwar einige Begrenzungen vor, die die Intensität des Eingriffs etwas abmildern. So begrenzt die Norm die Maßnahme in zeitlich-räumlicher Hinsicht. Sie erlaubt zudem lediglich die Suche nach bestimmten Personen. Im Vergleich zu den zuvor genannten Gesichtspunkten fallen diese Einschränkungen jedoch nicht entscheidend ins Gewicht, sodass gleichwohl ein Eingriff mit besonders hoher Intensität vorliegt.

Der Auffassung aus der Datenschutzfolgenabschätzung, dass es eingriffsmildernd wirke, dass außer den Systemanwendenden, die das VAS Videmo360 einsetzen, niemand die be-

troffenen Personen wahrnehmen würde (vgl. DSFA, Anlage B7, S. 70), kann nicht gefolgt werden. Das Polizeipräsidium Frankfurt am Main behält sich ausweislich der Datenschutzfolgenabschätzung vor, die im Rahmen der Maßnahme gewonnenen Erkenntnisse an zahlreiche weitere Behörden weiterzuleiten – etwa zur Strafverfolgung, für Strafverfahren oder zu sonstigen Zwecken der Gefahrenabwehr,

vgl. DSFA, Anlage B7, S. 46 ff.

Damit ist der Kreis derjenigen, denen die erfassten Daten zugänglich werden können, nicht auf die unmittelbaren Systemanwender beschränkt und führt zu keiner Milderung der Eingriffsintensität.

Ebenfalls nicht zu überzeugen vermag die Einschätzung in der Datenschutzfolgenabschätzung, es sei als eingriffsmildernd zu berücksichtigen, dass die gesuchten Personen zwingend einem qualifizierten Veranlassungszusammenhang unterlägen,

vgl. DSFA, Anlage B7, S. 69 f.

Diese Bewertung trifft schon tatbestandlich nicht in jedem Fall zu. Insbesondere bei der Suche nach vermissten Minderjährigen liegt nicht zwangsläufig eine Gefahrenlage vor, die einen solchen Veranlassungszusammenhang begründet (dazu unter bb)(2)(b)). Das Polizeipräsidium Frankfurt am Main räumt in seiner Datenschutzfolgenabschätzung selbst ein, dass im Falle einer Suche nach vermissten Personen, diese nur „u.U." nicht vernünftig die Folgen ihres Verhaltens bewerten und entsprechend eigenverantwortlich handeln könnten,

vgl DSFA, Anlage B7, S. 70.

Die zuständige Polizeibehörde geht damit selbst davon aus, dass der von ihr angeführte Veranlassungszusammenhang lediglich auf einer pauschalen Annahme beruht, die im Einzelfall nicht zutreffen muss.

Darüber hinaus wirkt sich lediglich potenziell eingriffsmildernd aus, dass die Daten bei einem Nicht-Treffer sofort wieder gelöscht werden. Zwar mag die eingesetzte Software ausweislich der Klageerwiderung auf diese Weise funktionieren (Klageerwiderung vom 17. Dezember 2025, S. 9). Die gesetzliche Grundlage sieht eine sofortige Löschung aber nicht vor.

§ 14 Abs. 9 – 11 HSOG könnte damit auch Grundlage für das Einsetzen einer Software sein, die die erhobenen Daten nicht direkt löscht. Solange eine entsprechende gesetzliche Absicherung fehlt, kann die behauptete Löschpraxis das Eingriffsgewicht nicht verlässlich mindern.

bb)Verstoß gegen das Gebot der Normenbestimmtheit und Normenklarheit

Der § 14 Abs. 9 – 11 HSOG stellt keine hinreichend bestimmte Ermächtigungsgrundlage dar, die einen derartigen Eingriff rechtfertigen kann.

(1) Verfassungsrechtlicher Maßstab

Grundrechtseinschränkungen sind nur wirksam, wenn sie unter Wahrung des Gesetzesvorbehalts normenklar und hinreichend bestimmt sind,

> BVerfG, Urteil vom 16. Februar 2023 - 1 BvR 1547/19 -, - 1 BvR 2634/20 -, Rn. 110 ff.

Das Gebot der Normenbestimmtheit stellt sicher, dass der demokratisch legitimierte Parlamentsgesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und ihre Reichweite selbst trifft, die Verwaltung steuernde und begrenzende Handlungsmaßstäbe vorfindet und die Gerichte eine wirksame Kontrolle durchführen können,

> BVerfGE 113, 348 (375ff.); 120, 378 (407); BVerfG, Urteil vom 01.10.2024 – 1 BvR 1160/19 -, NVwZ 2024, 1736 (1741).

Beim Gebot der Normenklarheit steht die inhaltliche Verständlichkeit einer Regelung im Vordergrund, insbesondere damit Bürger*innen sich auf mögliche belastende Maßnahmen einstellen können,

> BVerfG, Beschluss vom 28. September 2022 - 1 BvR 2354/13 -, NVwZ-RR 2023, 1 (6 Rn. 110); Hofmann, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 15. Aufl. 2022, Art. 20 Rn. 89, 91.

In Hinblick auf die Rolle, die das Gebot der Normenbestimmtheit zur Bindung der Verwaltung spielt, führt das Bundesverfassungsgericht aus:

> *„Die Anforderungen an die Bestimmtheit und Klarheit der Norm dienen auch dazu, die Verwaltung zu binden und ihr Verhalten nach Inhalt, Zweck und Ausmaß zu begrenzen (vgl. BVerfGE 56, 1 (12); stRspr). Dazu gehört, dass hinreichend klare Maßstäbe für Abwägungsentscheidungen bereitgestellt werden. Die Entscheidung über die Grenzen der Freiheit des Bürgers darf nicht einseitig in das Ermessen der Verwaltung gestellt sein (vgl. BVerfGE 78, 214 (226)). Dem Gesetz kommt im Hinblick auf den Handlungsspielraum der Exekutive eine begrenzende Funktion zu, die rechtmäßiges Handeln des Staates sichern und dadurch auch die Freiheit der Bürger vor staatlichem Missbrauch schützen soll. Dieser Aspekt der Bindung der Verwaltung ist bei einer Überwachungsmaßnahme besonders wichtig, da der Betroffene von ihr keine Kenntnis hat. Dies gilt insbesondere für unbeteiligte Dritte, die mit einer staatlichen Überwachung nicht rechnen und sich deshalb vor einem Einblick in ihren Privatbereich nicht schützen können“*
>
> BVerfGE 110, 33 (53 ff.).

In der verfassungsgerichtlichen Rechtsprechung haben sich im Laufe der Zeit greifbare Anforderungen an die Bestimmtheit von Ermächtigungsgrundlagen für staatliche Überwachungsmaßnahmen mit Eingriffscharakter entwickelt. Diese tragen dem allgemeinen Grundsatz Rechnung, wonach die Intensität eines Grundrechtseingriffs dafür maßgeblich ist, wie hoch die Anforderungen an die Bestimmtheit einer Norm sind. Gemeinhin gilt: Je bedeutsamer die Norm ist, insbesondere je intensiver die damit verbundene Freiheitseinschränkung des Bürgers ausfällt, desto höher ist das Maß der gebotenen inhaltlichen Bestimmtheit der Norm,

> BVerfG, Beschluss vom 8.08.1978 - 2 BvL 8/77 -, NJW 1979, 359 (360); grundlegend Grzeszick, in: Dürig/Herzog/Scholz, Grundgesetz, 106. EL Oktober 2024, Art. 20 Rn. 58 ff.

Hinsichtlich polizeibehördlicher Überwachungsmaßnahmen bedeutet das, dass Regelungen so bestimmt zu fassen sind, wie dies nach Eigenart des zu ordnendes Lebenssachverhalts

mit Rücksicht auf den Normzweck möglich ist. Es genügt dabei zwar, wenn sich durch Auslegung nach den allgemeinen Auslegungsregeln feststellen lässt, ob die tatsächlichen Voraussetzungen der Ermächtigungsgrundlage vorliegen. Allerdings dürfen verbleibende Unsicherheiten auch nicht so weit gehen, dass Vorhersehbarkeit und Justiziabilität des Handelns der durch die Norm ermächtigten staatlichen Stellen gefährdet sind,

> BVerfG, Urteil vom 01.10.2024 – 1 BvR 1160/19 -, NVwZ 2024, 1736 (1741).

Bei heimlicher Datenerhebung und -verarbeitung sind an die Bestimmtheit besonders strenge Anforderungen zu stellen:

> *„Dies trägt dem Umstand Rechnung, dass ein effektiver Schutz gegenüber staatlicher Datenerhebung und -verarbeitung nur auf Grundlage eines ausreichend spezifischen gesetzlichen Normprogramms möglich ist. Heimliche Überwachungsmaßnahmen gelangen den Betroffenen kaum zur Kenntnis und können daher von ihnen nur selten im Rechtsweg angegriffen werden. Der Gehalt der gesetzlichen Regelung kann so nur eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden, was der Gesetzgeber durch die hinreichende Bestimmtheit der jeweiligen Normen auffangen muss […]“,*
>
> BVerfG, Urteil vom 01.10.2024 - 1 BvR 1160/19 -, NVwZ 2024, 1736 (1741).

(2) Verstoß gegen verfassungsrechtliche Anforderungen

Diesen hohen Anforderungen an die Bestimmtheit und Normenklarheit genügt die Norm nicht. Es ist nicht hinreichend klar und bestimmt geregelt, welche Personen unter welchen konkreten Voraussetzungen mit einer Maßnahme nach § 14 Abs. 9 S. 2 HSOG gesucht werden können (dazu unter (i) und (ii). Darüber hinaus fehlen wesentliche Vorgaben für die Festlegung einer Mindestähnlichkeitsschwelle (dazu unter (iii)).

i. Opfer von Entführung, Menschenhandel oder sexuelle Ausbeutung

§ 14 Abs. 9 S. 2 HSOG spricht allgemein von „Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung“ und übernimmt dabei wortgetreu die Formulierung, die in Art. 5 Abs. 1 lit. h KI-VO gewählt wurde. Es ist davon auszugehen, dass mit der Formulierung „Opfer“ Geschädigte von Straftaten und/oder diejenigen Personen gemeint sind, die durch Straftaten in ihren Rechtsgütern unmittelbar betroffen sind. Es wird jedoch nicht weiter konkretisiert, welche konkreten Straftatbestände oder Begehungsformen aus dem Strafgesetzbuch von § 14 Abs. 9 S. 2 HSOG erfasst werden.

Während Menschenhandel in § 232 StGB normiert ist, gibt es im deutschen Strafgesetzbuch keinen entsprechenden Straftatbestand der Entführung. Der Begriff der „Entführung“ findet sich hingegen in verschiedenen Strafnormen, etwa in § 234b Abs. 1 Nr. 1 Fall 1 StGB, § 239a Abs. 1 Fall 1 StGB und § 239b Abs. 1 Fall 1 StGB. Im Sinne dieser Normen bedeutet „Entführen“ die Verbringung des Opfers gegen dessen Willen an einen anderen Ort, an dem es dem uneingeschränkten Einfluss des Täters ausgesetzt ist,

> Heger, in: Lackner/Kühl/Heger, StGB, 30.A. 2023, § 239a Rn. 3.

Unklar ist dann aber, ob sich auch andere Begehungsformen desselben Straftatbestandes, wie etwa das „sich bemächtigen“ nach § 239a Abs. 1 Alt. 2 StGB – das keine Ortsveränderung voraussetzt, in seinen Wirkungen auf das Opfer aber sonst keinen Unterschied macht – von § 14 Abs. 9 S. 2 HSOG erfasst werden. Darüber hinaus können auch bestimmte Begehungsformen der Freiheitsberaubung nach § 239 Abs. 1 Fall 2 StGB unter den allgemeinen Begriff der „Entführung“ subsumiert werden. Hier ist ebenso nicht hinreichend bestimmt, ob auch andere, gleichwertige Tatbestandsvarianten des § 239 Abs. 1 StGB erfasst sind – namentlich das Einsperren – oder eine Ortsveränderung zwingende Tatbestandsvoraussetzung der Norm ist.

Auch ein eigenständiger Straftatbestand der „sexuellen Ausbeutung“ existiert im deutschen Strafrecht nicht. Der Begriff „sexuelle Ausbeutung“ ist gesetzlich nicht näher ausgeformt und weist daher erhebliche Unschärfen auf. Sein Bedeutungsgehalt hängt stark von dem eigenen Begriffsverständnis der jeweils zuständigen Polizeibehörde ab, sodass ein weiter Interpretationsspielraum hinsichtlich der erfassten Delikte besteht.

Einige Gefahrenabwehrbehörden fassen darunter etwa neben Menschenhandel (§ 232 StGB), Zwangsprostitution (§ 232a StGB), Ausbeutung unter Ausnutzung einer Freiheitsberaubung (§ 233a StGB), Ausbeutung von Prostituierten (§ 180a StGB) und Zuhälterei (§ 181a StGB) – die im Wortlaut an eine „Ausbeutung“ anknüpfen – auch den sexuellen Missbrauch von Jugendlichen (§ 182 Abs. 2 StGB), den sexuellen Missbrauch von Kindern (§ 176 StGB und § 176a StGB) und die Förderung sexueller Handlungen Minderjähriger (§ 180 StGB),

> Landeskriminalamt NRW, Lagebild Menschenhandel und Ausbeutung, 2024, S. 4, abrufbar unter https://polizei.nrw/sites/default/files/2025-12/2025-12-15_Lagebild_Menschandel_und_Ausbeutung_2024.pdf (Letzter Abruf: 27.01.2026); Bundeskriminalamt, Bundeslagebild Sexualdelikte zum Nachteil von Kindern und Jugendlichen, 2023, abrufbar unter https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/SexualdeliktezNvKindernuJugendlichen/2023/BLBSexualdelikte_2023_node.html (Letzter Abruf: 27.01.2026)

Dahingegen geht das Übereinkommen des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (sog. „Lanzarote-Konvention“) von einer weiteren Definition aus und erfasst in Bezug auf Kinder alle Handlungen in Verbindung mit sexuellem Missbrauch, Straftaten im Zusammenhang mit Kinderprostitution, Straftaten im Zusammenhang mit Missbrauchsdarstellungen von Kindern („Kinderpornographie“), Straftaten betreffend die Mitwirkung eines Kindes an pornographischen Darbietungen, das vorsätzliche Veranlassen eines Kindes, bei sexuellen Handlungen zugegen zu sein, und Kontaktanbahnung zu Kindern zu sexuellen Zwecken (sog. „Grooming“) (Art. 3 lit. b i.V.m. Art. 18 - 23 der Konvention).

> Vgl. Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeu tung und sexuellem Missbrauch, S. 4, 11 ff., abrufbar unter https://rm.coe.int/ CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=090000168046e1ea – zuletzt abgerufen am 21.04.2026.

Nach dieser Definition fielen auch Kinder und Jugendliche, die Opfer von Straftaten nach § 184b StGB und § 184c StGB unter den Begriff Opfer sexueller Ausbeutung.

In der Wissenschaft wird der Begriff der sexuellen Ausbeutung noch weiter gefasst. Sexuelle Ausbeutung ist demnach

> *„jeder tatsächliche oder versuchte Missbrauch einer Situation der Verletzlichkeit, unterschiedlicher Macht oder von Vertrauen für sexuelle Zwecke, einschließlich, aber nicht hierauf beschränkt, des finanziellen, sozialen oder politischen Profitierens von der sexuellen Ausbeutung anderer“*
>
> European Institute for Gender Equality, Glossary and Thesaurus, Sexuelle Ausbeutung, Abrufbar unter https://eige.europa.eu/publications-resources/thesaurus/terms/1188?language_content_entity=de (Letzter Abruf: 27.01.2026).

Nach dieser Definition sind Fälle sexueller Ausbeutung denkbar, die nicht von den aufgelisteten Straftatbeständen erfasst sind, aber etwa eine Nötigung (§§ 240 Abs. 1, 2 StGB) oder versuchte Nötigung (§§ 240 Abs. 3, 22 StGB) darstellen.

Unklar ist darüber hinaus auch, welchen Grad an Gewissheit die Norm erfordert, um eine bestimmte Person als „Opfer“ einer Straftat einzuordnen. § 14 Abs. 9 S. 2 HSOG trifft keine Regelung dazu, ob bereits eine Strafanzeige oder ein Anfangsverdacht hinsichtlich einer bestimmten Straftat ausreichend ist oder ein darüber hinausgehender Verdachtsgrad erforderlich ist. § 14 Abs. 9 S. 2 HSOG lässt damit sowohl hinsichtlich der erfassten Straftaten und Gefahrenlagen als auch hinsichtlich der erforderlichen Eingriffsschwelle und des maßgeblichen Zeitpunkts des Einsatzes die verfassungsrechtlich gebotene Normenbestimmtheit und Normenklarheit vermissen. Dies hat zur Folge, dass weder die rechtsanwendende Behörde hinreichend klare Handlungsmaßstäbe vorfindet noch für Betroffene erkennbar ist, unter welchen Voraussetzungen sie mit einer solchen Maßnahme rechnen müssen.

Auch wenn die Pilotphase des polizeilichen Projekts ausweislich der Klageerwiderung sich auf die gezielte Suche auf vermisst gemeldete Minderjährige sowie Gefahrenverursacher terroristischer Straftaten konzentriere (Klageerwiderung vom 17. Dezember 2025, S. 4), ist nicht ausgeschlossen, dass die Polizei die Maßnahme derzeit auch zur Suche nach Opfern

von Entführung, Menschenhandel und sexueller Ausbeutung einsetzt und zukünftig einsetzen wird. Dies ergibt sich insbesondere aus den Ausführungen in der Datenschutzfolgeabschätzung, wonach der Polizeibehörde die Erstreckung der gezielten Suche auf andere in § 14 Abs. 9 Satz 2 HSOG benannte Personengruppen dabei je nach einzelfallorientierter Lagebeurteilung vorbehalten bleibe,

vgl. DSFA, Anlage B7, S. 6 f.

ii. Vermisste Personen

Hinsichtlich der Suche nach vermissten Personen enthält § 14 Abs. 9 S. 2 HSOG gleichermaßen keine Regelung, die hinreichend bestimmte Eingriffsschwellen oder tatbestandliche Voraussetzungen für die Maßnahme festlegt. Einzig normierte Voraussetzung ist, dass eine Person im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme als vermisst gespeichert ist und die Suche nach dieser Person auf diese Weise unbedingt erforderlich ist. Der Gesetzestext enthält weder die Vorgabe, dass eine Gefahr für bestimmte Rechtsgüter tatsächlich vorliegen muss, noch Regelungen zur erforderlichen Gefahrenschwelle oder dazu, welcher Grad an Gewissheit hinsichtlich einer Gefahrenlage erforderlich ist und welche Rechtsgüter konkret gefährdet sein müssen. Ebenso wenig wird geregelt, ob und unter welchen Voraussetzungen die Maßnahme bei einer als vermisst gemeldeten Person zulässig sein soll, die freiwillig untergetaucht ist und keiner Gefahr ausgesetzt ist. Das zeigt sich insbesondere daran, dass unterschiedliche Anforderungen an die Aufnahme von vermisst gemeldeten Erwachsenen und Minderjährigen in das polizeiliche Fahndungssystem gestellt werden.

Ausweislich der Informationen des Bundeskriminalamts leitet die Polizei bei Erwachsenen eine Vermissten-Fahndung ein, wenn die Person ihren gewohnten Lebenskreis verlassen hat, ihr derzeitiger Aufenthalt unbekannt ist und eine Gefahr für Leib oder Leben (z.B. Opfer einer Straftat, Unfall, Hilflosigkeit, Selbsttötungsabsicht) aufgrund tatsächlicher, ihr vorliegender Anhaltspunkte angenommen werden kann. Dahingegen werden als vermisst gemeldete minderjährige Personen bereits in das polizeiliche Fahndungssystem aufgenommen, wenn sie ihren gewohnten Lebenskreis verlassen haben und ihr Aufenthalt nicht bekannt ist. Objektive Anhaltspunkte für eine Gefahrenlage müssen nicht vorliegen. Da Minderjährige

ihren Aufenthaltsort nicht selbst bestimmen dürfen, geht die Polizei in diesen Fällen „vorsichtshalber von einer Gefahr für das Leben und körperliche Unversehrtheit des Betroffenen aus", solange die Ermittlungen nichts anderes ergeben,

> vgl. BKA, Die polizeiliche Bearbeitung von Vermisstenfällen in Deutschland, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/BearbeitungVermisstenfaelle/bearbeitungVermisstenfaelle.html?nn=30666#doc19618bodyText1 (Letzter Abruf: 13. April 2026).

Dass diese pauschale Annahme einer Gefahrenlage bei Minderjährigen jedoch keineswegs der tatsächlichen Sachlage entspricht, belegen die Angaben des Bundeskriminalamts zur Zusammensetzung der als vermisst gespeicherten Personen. Danach machen etwa zwei Drittel der als vermisst gespeicherten Kinder bis einschließlich 13 Jahren unbegleitete Geflüchtete, sogenannte Dauerausreißer und Streunende oder Kinder, die einem Sorgeberechtigten entzogen wurden, aus (Stand: 1. Januar 2026),

> vgl. BKA, Die polizeiliche Bearbeitung von Vermisstenfällen in Deutschland, a.a.O.

In diesen Kategorien ist jedoch häufig keine tatsächliche Gefahr für Leib oder Leben der vermissten Person gegeben. In Fällen der Kindesentziehung, deren Hintergrund Streitigkeiten der Eltern über die Ausübung des Sorgerechts sind, bestehe nach eigenen Angaben des Bundeskriminalamts

> *„in aller Regel* [...] *in diesen Fällen jedoch keine Gefahr für die Kinder, da sie sich während ihrer ‚Abwesenheit' in der Obhut eines Erwachsenen befinden, zu dem sie eine enge Bindung haben",*
>
> BKA, Die polizeiliche Bearbeitung von Vermisstenfällen in Deutschland, a.a.O.

Gleichwohl werden auch solche Fälle zunächst als Vermisstenfälle im polizeilichen Fahndungssystem erfasst, solange eine Gefahr für die betroffenen Kinder nicht mit Sicherheit ausgeschlossen werden kann.

Entsprechendes gilt für unbegleitete Geflüchtete, bei denen das Verschwinden ebenfalls typischerweise nicht auf einer Gefährdung von Leib oder Leben beruht. Das Bundeskriminalamt nennt als häufigste Ursache für ihr Verschwinden das freiwillige Verlassen zugewiesener Unterkünfte, um Familienangehörige oder Bekannte im Ausland aufzusuchen oder ins Herkunftsland zurückzukehren,

> BKA, Die polizeiliche Bearbeitung von Vermisstenfällen in Deutschland, a.a.O.

In diesen Fällen handelt es sich gerade nicht um ein unfreiwilliges Verschwinden oder eine Situation, in der die betroffene Person einer akuten Gefährdung ausgesetzt ist, sondern um eine eigenständige, bewusste Entscheidung, den zugewiesenen Aufenthaltsort zu verlassen. Eine Gefahr für Leib oder Leben ist damit von vornherein nicht Ursache des Verschwindens, sondern allenfalls abstrakt denkbar und nur beim Vorliegen zusätzlicher Umstände möglicherweise gegeben, die aber auch tatsächlich festgestellt werden müssten.

Bei „Dauerausreißern“ und „Streunenden“ handelt es sich um Minderjährige, die wiederholt und über längere Zeiträume in der Regel aus eigenem Antrieb ihren gewohnten Lebenskreis verlassen, ohne dass dies zwingend auf eine akute Gefahrenlage hindeutet. Auch hier erfolgt die Aufnahme in das Fahndungssystem pauschal und ohne konkrete Feststellung einer Gefährdung – allein aufgrund des Umstands, dass der Aufenthaltsort unbekannt ist.

Hinzu kommt, dass § 14 Abs. 9 S. 2 HSOG auch innerhalb der Gruppe der Minderjährigen keine Differenzierung nach Alter sowie geistiger und körperlicher Reife vorsieht. Diese Faktoren sind jedoch neben den konkreten Umständen des Verschwindens wesentlich für die Beurteilung einer tatsächlichen Gefahrenlage. Die Einschätzung, ob eine konkrete Gefährdung vorliegt, unterscheidet sich erheblich danach, ob es sich um ein zehnjähriges Kind oder einen bereits 17-jährigen Jugendlichen handelt, der eigenverantwortlich handeln kann und dessen Verschwinden auf einem freien Entschluss beruhen mag. Eine Norm, die diese Unterschiede vollständig ausblendet und allein auf die Tatsache der Vermisstenmeldung abstellt, wird den verfassungsrechtlichen Anforderungen an eine hinreichend bestimmte Eingriffsschwelle nicht gerecht.

Darüber hinaus ist die Ermächtigungsgrundlage auch in zeitlicher Hinsicht nicht hinreichend begrenzt. Im polizeilichen Fahndungssystem „INPOL“ sind nach Angaben des Bundeskriminalamts auch Fälle gespeichert, in denen eine Person seit vielen Jahren oder sogar Jahrzehnten als vermisst gilt und deren Aufenthaltsort oder Verbleib bis heute nicht festgestellt werden konnte. Wird eine Vermisstensache nicht aufgeklärt, bleibt die Personenfahndung nach den Angaben des Bundeskriminalamts bis auf Widerruf bestehen,

> vgl. BKA, Die polizeiliche Bearbeitung von Vermisstenfällen in Deutschland, a.a.O.

Da § 14 Abs. 9 S. 2 HSOG keine zeitliche Begrenzung für die Zulässigkeit der Maßnahme enthält und allein auf die Speicherung im Fahndungssystem abstellt, wäre die biometrische Echtzeit-Fernidentifizierung nach dem Gesetzeswortlaut auch dann zulässig, wenn eine Person seit Jahren oder Jahrzehnten als vermisst gilt und keine aktuellen Anhaltspunkte für eine fortbestehende Gefahrenlage vorliegen. Da die Norm die zeitliche Reichweite der Vermissteneigenschaft vollständig ungeregelt lässt, genügt sie auch insoweit den verfassungsrechtlichen Anforderungen an eine hinreichend bestimmte Rechtsgrundlage nicht.

Vor diesem Hintergrund überzeugt die Auffassung des Beklagten, dass bei vermissten Minderjährigen stets von einer konkreten Beeinträchtigung in Form von Misshandlungen, Missbrauch oder sexueller Ausbeutung auszugehen sei (Klageerwiderung vom 17. Dezember 2025, S. 7), nicht. Sie verkennt bereits den systematischen Aufbau der Norm: § 14 Abs. 9 S. 2 HSOG zählt die Suche nach vermissten Personen ausdrücklich als eigenständige, neben der Suche nach Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung stehende Kategorie auf. Wären vermisste Minderjährige stets zugleich Opfer sexueller Ausbeutung oder einer vergleichbaren Straftat, bedürfte es dieser eigenständigen Kategorie nicht. Die Norm erlaubt den Einsatz der Maßnahme bei vermissten Personen mithin gerade unabhängig vom Vorliegen einer solchen konkreten Gefährdung.

Zwar trifft es zu, dass bestimmte Gefahrenlagen – insbesondere Misshandlungen, Missbrauch oder sexuelle Ausbeutung – langfristige und tiefgreifende Folgen für die Persönlichkeitsentwicklung haben können, bis hin zu lebenslangen Traumata und Körperschäden. Dies

ändert jedoch nichts daran, dass eine solche Gefahrenlage nicht allein aufgrund einer Vermisstenmeldung als vorliegend angenommen werden kann.

§ 14 Abs. 9 S. 2 HSOG enthält damit keine hinreichend bestimmte Eingrenzung auf Vermisstenfälle, in denen eine tatsächliche Gefahrenlage für ein konkret benanntes Schutzgut angenommen werden kann sowie keine Festlegung konkreter Gefahrenschwellen und Eingriffsvoraussetzungen, die dem besonders hohen Eingriffsgewicht hinreichend Rechnung tragen. So geht auch die Annahme in der Datenschutzfolgenabschätzung fehl, wonach die gesuchten Personen zwingend einem qualifizierten Veranlassungszusammenhang unterlägen,

vgl. DSFA, Anlage B7, S. 69 f.

Der Gesetzgeber ist angehalten, durch hinreichend bestimmte tatbestandliche Voraussetzungen gesetzlich sicherzustellen, dass die Maßnahme nur in solchen Fällen eingesetzt werden darf, in denen tatsächlich konkrete Anhaltspunkte für eine Gefährdung von hinreichend gewichtigen Rechtsgütern vorliegen – differenziert nach Alter und Reife der vermissten Person, den konkreten Umständen des Verschwindens sowie dem Grad der tatsächlich feststellbaren Gefahrenlage.

iii. Fehlende verbindliche Vorgaben zur Festlegung der Mindestähnlichkeitsschwelle

Durch die fehlende gesetzliche Vorgabe eine beim Einsatz der biometrischen Echtzeit-Fernidentifizierung verbindliche Mindestähnlichkeitsschwelle zu regeln, anhand derer das eingesetzte VAS Videmo360 die biometrischen Daten mit dem Referenzmaterial abgleicht, werden die verfassungsrechtlichen Anforderungen an Normenbestimmtheit und Normenklarheit unterschritten.

Ausweislich der Klageerwiderung sowie der Datenschutz- und Grundrechtefolgenabschätzung (Klageerwiderung vom 17. Dezember 2025, S. 9, Anlage B7, S. 8 f., 12) legen die zuständigen Polizeibeamt:innen diese Schwelle bei jedem Einsatz nach freiem Ermessen selbst fest.

Die Mindestähnlichkeitsschwelle ist dabei keine technische Nebensächlichkeit, sondern als eine wesentliche grundrechtsrelevante Entscheidung einzustufen, die durch den Gesetzgeber selbst hinreichend klar geregelt werden muss. Denn der eingestellte Mindestähnlichkeitswert bestimmt unmittelbar, wie viele Personen im Erfassungsbereich der Kamera als potenzielle Treffer erfasst, ihre biometrischen Daten abgeglichen und damit einer längerfristigen Speicherung ihrer Daten, polizeilichen Anschlussmaßnahmen sowie einem Fehlidentifikationsrisiko ausgesetzt werden.

Das Bundesverfassungsgericht hat klargestellt, dass das Gebot der Normenbestimmtheit gerade bei heimlichen Überwachungsmaßnahmen erfordert, dass

> *„hinreichend klare Maßstäbe für Abwägungsentscheidungen bereitgestellt werden"* [und] *„die Entscheidung über die Grenzen der Freiheit des Bürgers nicht einseitig in das Ermessen der Verwaltung gestellt sein“* [darf],
>
> BVerfG, Beschluss vom 3. März 2004 - 1 BvF 3/92, NJW 2004, 2213 (2216).

Diesen Anforderungen genügt § 14 Abs. 9 - 11 HSOG nicht. Die Norm überlässt die Festlegung einer der eingriffsrelevantesten Parameter des Einsatzes der biometrischen Echtzeit-Fernidentifizierung vollständig dem Ermessen der handelnden Behörde und sieht weder gesetzliche Mindest- oder Höchstvorgaben noch Begründungspflichten gegenüber dem Gericht oder effektive Kontrollmöglichkeit für die Betroffenen vor. Damit fehlt es an der von der Wesentlichkeitstheorie geforderten parlamentarischen Vorentscheidung über die Reichweite und Grenzen des Eingriffs

cc) Unverhältnismäßigkeit

Der Eingriff greift in unverhältnismäßiger Weise in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein.

(1) Legitimer Zweck

Der Eingriff dient zunächst einem legitimen Zweck. § 14 Abs. 9 S. 1 HSOG dient der Abwehr terroristischer Gefahren. Potenzielle Täter terroristischer Straftaten sollen erkannt und so die Grundlage für gefahrenabwehrrechtliche Folgemaßnahmen geschaffen werden. § 14 Abs. 9 S. 2 HSOG dient dem Auffinden von Opfern von Straftaten, die mit einer konkreten oder zumindest abstrakten Gefährdung von Leib, Leben, Freiheit und sexueller Selbstbestimmung einhergehen.

(2) Geeignetheit

Die Einräumung der Befugnisse ist zur Erreichung des Zwecks geeignet. Mithilfe des Datenbankabgleichs besteht zumindest die Möglichkeit, dass die betroffenen Personen „in Echtzeit“ gefunden werden.

(3) Erforderlichkeit

Die Befugnisse sind nur zum Teil erforderlich. Für die gezielte Suche nach Opfern von Entführung, Menschenhandel und sexueller Ausbeutung sowie von vermissten Personen nach § 14 Abs. 9 S. 2 HSOG stehen mildere, gleich wirksame Mittel zur Verfügung, insbesondere die Mobilfunkortung.

Die Einschätzung in der Datenschutzfolgenabschätzung, dass die Mobilfunkortung als milderes Mittel ausscheide (DSFA, Anlage B7, S. 61), vermag nicht zu überzeugen. Zum einen trägt der dortige Einwand nicht, dass mit der Mobilfunkortung ein Eingriff in das Fernmeldegeheimnis aus Art. 10 GG im Raum stehe. Da die Mobilfunkortung ausschließlich die jeweils gesuchte Person betrifft und die massenhafte verdeckte biometrische Erfassung Unbeteiligter mittels eines fehler- und diskriminierungsanfälligen KI-Systems vermeidet, wäre ein dabei möglicher Eingriff in das Fernmeldegeheimnis weniger eingriffsintensiv. Der weitere Einwand aus der Datenschutzfolgenabschätzung, die gesuchte Person könne kein Mobiltelefon bei sich führen (DSFA, Anlage B7, S. 61), betrifft allenfalls Einzelfälle und schließt die Mobilfunkortung nicht generell als milderes Mittel aus. Insbesondere bei vermissten Minderjährigen entspricht es der Lebenswirklichkeit, dass diese typischerweise ein Mobiltelefon bei

sich tragen. Für diese Fallgruppe wäre die Mobilfunkortung daher regelmäßig verfügbar. Schließlich wird in der Datenschutzfolgenabschätzung eine solche Maßnahme als milderes Mittel mit dem Argument ausgeschlossen, dass Verdächtige ihre Mobiltelefone erfahrungsgemäß zu Hause lassen,

vgl. DSFA, Anlage B7, S. 61.

Dies bezieht sich jedoch allein auf Konstellationen des § 14 Abs. 9 S. 1 HSOG, in dem Terrorismusverdächtige gezielt einer Identifizierung ausweichen wollen. Auf vermisste Personen und Opfer von Straftaten nach § 14 Abs. 9 S. 2 HSOG ist es dahingegen nicht übertragbar.

Auch für die Suche nach Personen nach § 14 Abs. 9 S. 1 HSOG kommt die Observation nach § 15 HSOG als milderes, gleich geeignetes Mittel in Betracht. Die Datenschutzfolgenabschätzung schließt die Observation aufgrund des hohen Personalaufwands und der Gefahr, entdeckt zu werden, als ungeeignet aus,

vgl. DSFA, Anlage B7, S. 62.

Die erste Erwägung betrifft jedoch nicht die (fehlende) Wirksamkeit der Observation, sondern allein ihre Ressourcenintensität. Dieser Aspekt ist jedoch im Rahmen der Erforderlichkeitsprüfung ohne Belang, da es allein darauf ankommt, ob der Einsatz eines anderen Mittels den Zweck der Maßnahme gleich wirksam erreichen kann.

Das Argument des Entdeckungsrisikos ist demgegenüber nicht auf konkrete tatsächliche Anhaltspunkte gestützt, sondern wird in der Datenschutzfolgenabschätzung lediglich pauschal behauptet. Gerade bei gut ausgebildeten Observationskräften ist eine generelle Annahme, die gesuchte Person werde die Observation bemerken, nicht belastbar.

Unabhängig davon geht die Maßnahme in ihrer konkreten normativen Ausgestaltung über das zur Zweckerreichung Erforderliche hinaus. Da die Rechtsgrundlage keine verbindliche Mindestähnlichkeitsschwelle vorschreibt und deren Festlegung dem freien Ermessen der handelnden Beamt:innen überlässt, erfasst die Maßnahme zwangsläufig mehr Personen als zur Identifizierung der jeweils gesuchten Person notwendig wäre (dazu bereits oben unter (2)(c)). Eine gesetzlich normierte Mindestschwelle, die den Kreis der als Treffer erfassten

Personen auf das unbedingt Erforderliche begrenzt, würde den Eingriff bei gleicher Wirksamkeit erheblich reduzieren. Das Fehlen einer solchen Vorgabe macht die Maßnahme in ihrer gegenwärtigen Ausgestaltung auch insoweit nicht erforderlich.

Schließlich geht die Maßnahme auch in zeitlicher Hinsicht über das Erforderliche hinaus. Die Rechtsgrundlage sieht — anders als vergleichbare verdeckte Maßnahmen nach §§ 15 ff. HSOG — keine gesetzliche Höchstfrist vor. Nach den Angaben in der Datenschutzfolgenabschätzung kann die Maßnahme bei jedem Einsatz für einen Zeitraum von bis zu drei Monaten angeordnet werden, der bei Folgeanträgen um weitere drei Monate verlängert werden kann,

vgl. DSFA, Anlage B7, S. 43, 67.

Eine solche Anordnungsdauer ist für die gezielte Suche nach einer bestimmten Person in der Regel weder notwendig noch auf das unbedingt erforderliche Maß beschränkt. Hinzu kommt, dass § 14 Abs. 9 S. 2 HSOG den Einsatz auch dann erlaubt, wenn die zugrundeliegende Straftat bereits länger zurückliegt und/oder keine akute Gefährdungslage mehr besteht (dazu oben unter (2)(b) sowie unter (4)(bb) und (cc)). Die Regelung einer hinreichend konkreten Gefahrenschwelle sowie eine gesetzlich normierte Höchstfrist mit engen Voraussetzungen für eine Verlängerung würde somit den Eingriff bei gleicher Wirksamkeit erheblich reduzieren.

(4) Angemessenheit

Allerdings ist der Eingriff nicht angemessen und damit nicht verhältnismäßig im engeren Sinn.

i. Verfassungsrechtlicher Maßstab

Greifen Maßnahmen der Gefahrabwehr in die informationelle Selbstbestimmung ein, geht die verfassungsgerichtliche Rechtsprechung von „sehr hohen Voraussetzungen“ aus, um die Verhältnismäßigkeit zu wahren,

> BVerfG, Urteil vom 27.05.2005 - 1 BvR 668/04 -, BVerfGE 113, 348 (386); vgl. auch BVerfG, Beschluss vom 4.04.2006 - 1 BvR 518/02 -, BVerfGE 115, 320, 360 ff.; BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07 und 1 BvR 595/07 -, BVerfGE 120, 274 (321); BVerfG, Urteil vom 2.03.2010 - 1 BvR 256/08 -, - 1 BvR 263/08 -, -1 BvR 586/08 -, BVerfGE 125, 260 (327ff. Rn. 225 ff.; 334 ff., Rn. 238 ff.; 340 ff., Rn. 254 ff.);

Eingriffe in das Grundrecht auf informationelle Selbstbestimmung mit einer derart besonders hohen Intensität sind nach verfassungsrechtlicher Rechtsprechung nur zum Schutz besonder gewichtiger Rechtsgüter zulässig,

> BVerfG Urteil vom 16. Februar 2023 - 1 BvR 1547/19 -, - 1 BvR 2634/20 -, NJW 2023, 1196 (1206 Rn. 105 m.w.N.).

Zu den besonders gewichtigen Rechtsgütern zählen vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes. Dabei kann der Gesetzgeber darauf verzichten, das erforderliche Rechtsgut unmittelbar zu benennen und stattdessen an entsprechende Straftaten anknüpfen, deren Verhütung mit der Befugnis bezweckt ist,

> BVerfG Urteil vom 16. Februar 2023 - 1 BvR 1547/19 -, - 1 BvR 2634/20 -, NJW 2023, 1196 (1206 Rn. 105 m.w.N.).

Zusätzlich gilt bei heimlichen Überwachungsmaßnahmen der Gefahrenabwehrbehörden allgemein das Erfordernis einer konkreten Gefahr. Diese Eingriffsschwelle kann auf eine hinreichend konkretisierte Gefahr abgesenkt werden, wenn dafür erhöhte Anforderungen an das geschützte Rechtsgut gestellt werden,

> BVerfG, Beschluss vom 24.06.2025 – 1 BvR 2466/19 – MMR, 2026, 44 (49 Rn. 129).

Eine hinreichend konkretisierte Gefahr setzt voraus, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen,

> BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19 und 1 BvR 2634/20 -, NJW 2023, 1196 (1206 Rn. 106).

ii. Unangemessene Gefahrenschwelle für die Suche nach Opfern von Entführung, Menschenhandel und sexueller Ausbeutung

§ 14 Abs. 9 S. 2 HSOG unterschreitet die verfassungsrechtlichen Anforderung, dass darauf gestützte Maßnahmen nur auf Fälle, in denen eine hinreichend konkretisierte Gefahr für das zu schützende Rechtsgut vorliegt, zu beschränken sind. Die Norm verlangt lediglich, dass die gesuchte Person als ein Opfer von Entführung, Menschenhandel oder sexueller Ausbeutung im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeichert ist und die Suche nach ihr auf diese Weise unbedingt erforderlich ist.

Allein die Eigenschaft als „Opfer“ bestimmter Straftaten – etwa nach § 232 StGB oder § 176 StGB – begründet jedoch nicht zwingend das Vorliegen einer konkreten Gefahr für die betroffenen Rechtsgüter. So umfasst etwa der § 232 Abs. 1 StGB auch Begehungsformen, in denen ein baldiger Schadenseintritt nicht unbedingt nötig ist und somit nicht zwingend eine Gefahr vorliegt. Grund dafür ist, dass § 232 StGB als abstraktes Gefährdungsdelikt ausgestaltet ist,

> *Eisele*, in: Tübinger Kommentar, 2025, § 232 Rn. 10.

Unter Strafe gestellt wird das Anwerben, Befördern, Weitergeben, Beherbergen und Aufnehmen einer anderen Person unter Ausnutzung ihrer persönlichen oder wirtschaftlichen Zwangslage, ihrer Hilfslosigkeit, die mit dem Aufenthalt in einem fremden Land verbunden ist, oder wenn das Opfer unter 21 Jahre alt ist – sofern es ausgebeutet werden soll. Weder muss eine Ausbeutung tatsächlich erfolgen, noch muss eine zumindest konkretisierte Gefahr für eine solche drohen. Damit kann die Maßnahme nach § 14 Abs. 9 – 11 HSOG auch im Vorfeld einer konkretisierten Gefahr eingesetzt werden und erfasst Fälle, in denen der Einsatz unverhältnismäßig wäre.

Auch in zeitlicher Hinsicht ist nicht zwingend von einer fortbestehenden Gefahr auszugehen. Denkbar ist, dass die Begehung der Straftat bereits einige Zeit zurück liegt. Dann ist die gesuchte Person zwar nach wie vor Geschädigte, und damit „Opfer“ der Straftat. Die betroffe-

ne Person bleibt zwar Geschädigte und damit „Opfer“ der Straftat; ihre Auffindung kann etwa für eine Zeug:innenvernehmung im Ermittlungsverfahren erforderlich sein. Eine gegenwärtige oder konkretisierte Gefahr für ein Schutzgut besteht in diesen Fällen jedoch nicht mehr.

Zudem werden bestimmte von der Rechtsgrundlage erfassten Straftaten wie §§ 184b, 184c StGB häufig nach der konkreten sexuellen Ausbeutung der abgebildeten Person begangen – indem die früher angefertigten Aufnahmen verbreitet, erworben oder besessen werden. Zu diesem Zeitpunkt können die abgebildeten Kinder und Jugendlichen nach wie vor konkret in Leib, Leben oder persönlicher Freiheit gefährdet sein. Liegt die Erstellung der Inhalte aber länger zurück, fehlt es regelmäßig an einer aktuellen Gefährdung dieser Rechtsgüter. Die Rechtsgrundlage in § 14 Abs. 9 – 11 HSOG erfasst aber auch diese Fälle und ermöglicht den Einsatz der Echtzeit-Fernidentifizierung auch Jahre nach der mutmaßlichen Tat, wenn keine Gefährdung (mehr) für die Rechtsgüter der betroffenen Person bestehen.

Schließlich fehlt es an einer hinreichend bestimmten und im Verhältnis zur besonders hohen Eingriffsintensität angemessenen Eingrenzung des Opferbegriffs. Die Norm regelt weder, ab welchem Verfahrensstadium noch mit welchem Gewissheitsgrad eine Person als „Opfer“ einer Straftat anzusehen ist. Der weite Wortlaut eröffnet vielmehr die Möglichkeit, bereits das eines bloßen Anfangsverdachts oder einer Strafanzeige genügen zu lassen und damit die Maßnahme bereits weit im Vorfeld einer zumindest konkretisierten Gefahr einzusetzen. Damit wird die Anwendbarkeit der Maßnahme von Voraussetzungen abhängig gemacht, die ihrerseits nicht notwendig das Bestehen einer konkreten oder zumindest hinreichend konkretisierten Gefahr für ein bestimmtes Schutzgut indizieren. Eine solche Ausgestaltung wird den verfassungsrechtlichen Anforderungen an die tatbestandliche Gefahrenschwelle nicht gerecht.

iii. Fehlende Gefahrenschwelle für Suche nach vermissten Personen im Gesetzestext

§ 14 Abs. 9 S. 2 HSOG unterschreitet die verfassungsrechtlichen Anforderungen an die tatbestandliche Gefahrenschwelle auch hinsichtlich der Suche nach vermissten Personen. Eine gesetzliche Vorgabe, dass zumindest eine konkretisierte Gefahr für ein bestimmtes Rechtsgut der zu suchenden vermissten Person vorliegen muss, fehlt.

„Vermisst“ ist grundsätzlich jede Person, deren Aufenthaltsort unbekannt ist und deren Wohlergehen von Dritten in Frage gestellt wird. Dies erfasst gleichermaßen:

- den demenzkranken Seniorenheimbewohner, der beim Spaziergang die Orientierung verloren hat,
- die volljährige Person, die sich bewusst und eigenverantwortlich aus ihrem sozialen Umfeld zurückgezogen hat,
- das Kind, das später als erwartet nach Hause kommt,
- die Person, die freiwillig und ohne Gefährdung für sich selbst untergetaucht ist.

Ob der angegebene Grund für die Besorgnis um das Wohlergehen objektiv begründet ist, dazu macht die Norm keinerlei Vorgaben. Die genannten Konstellationen unterscheiden sich auch erheblich hinsichtlich der Notwendigkeit, die mittels biometrischer Echtzeitidentifizierung durchzuführen. Die Norm lässt hier tatbestandlich gleichermaßen den Einsatz biometrischer Echtzeit-Fernidentifizierung zu, ohne dass eine konkret definierte Gefahrenschwelle zu überwinden wäre. Wer als „vermisst“ gilt und damit zum tauglichen Ziel biometrischer Echtzeit-Überwachung wird, bestimmt sich letztlich anhand einer nicht durch konkrete Tatbestandsmerkmale umgrenzten Einschätzung der handelnden Beamt:innen.

Wie bereits im Rahmen des Verstoßes gegen das Gebot der Normenbestimmtheit und Normenklarheit umfassend ausgeführt, erlaubt die Ermächtigungsgrundlage durch die alleinige Anknüpfung an die Vermissteneigenschaft einer Person – insbesondere bei Minderjährigen – den Einsatz der biometrischen Echtzeit-Fernidentifizierung auch in Fällen, in denen keine Gefahrenlage bzw. keine konkretisierte Gefahr für ein Rechtsgut der vermissten Person vorliegt (siehe dazu oben bb)(2)(b)). Das Bundesverfassungsgericht hat zu den Anforderungen an die Gefahrenschwelle bei besonders eingriffsintensiven heimlichen Überwachungsmaßnahmen ausgeführt, dass die Gefahrenprognose ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennen lassen muss und sich nicht allein auf allgemeine Erfahrungssätze stützen darf,

> BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1791).

Vielmehr müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen,

> BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1206 Rn. 106).

Die tatbestandliche Ausgestaltung des § 14 Abs. 9 S. 2 HSOG lässt es hingegen zu, allein an den Umstand anzuknüpfen, dass eine minderjährige Person im polizeilichen Fahndungssystem als vermisst gespeichert ist – und damit an die pauschale, auf allgemeinen Erfahrungssätzen gestützte polizeiliche Annahme, dass damit zugleich eine Gefahr für Leib und Leben dieser Person vorliege (vgl. dazu oben bb)(2)(b)). Damit gibt die Ermächtigungsgrundlage den Behörden und Gerichten keine hinreichend bestimmten Kriterien an die Hand, eröffnet Maßnahmen, die unverhältnismäßig weit sein können, und wird den verfassungsrechtlichen Anforderungen an die tatbestandliche Gefahrenschwelle nicht gerecht.

iv. Unangemessene Gefahrenschwelle in § 14 Abs. 9 S. 1 HSOG

Nach § 19 Abs. 9 S. 1 HSOG soll eine „tatsächliche und bestehende oder tatsächliche und vorhersehbare Gefahr einer terroristischen Straftat“ erforderlich sein, um eine biometrische Echtzeit-Fernidentifizierung vornehmen zu dürfen. Diese Gefahrenschwellen sind im deutschen Polizeirecht unbekannt und wurden offenbar aus der KI-VO übernommen. Sie sind in mehrfacher Hinsicht unangemessen.

Die Norm stellt zwei Gefahrenkategorien nebeneinander: die „tatsächliche und bestehende Gefahr" sowie die „tatsächliche und vorhersehbare Gefahr". Beide Gefahrenstufen sind durch die polizeirechtliche Judikatur nicht näher konturiert. Während eine „bestehende Gefahr“ nahe der „konkreten Gefahr“ zu verorten sein dürfte, ist völlig unklar, wann eine Gefahr „vorhersehbar“ sein soll,

> vgl. auch *Töpfer/Kleemann*, Polizeiliche Gesichtserkennung: Menschenrechtliche Herausforderungen einer Risikotechnologie, 2025, S. 31.

Dieser bezieht sich auf Gefahren, die nicht konkret bestehen, sondern möglicherweise entstehen können, also auf abstrakte Gefahren. Die Norm verlagert die Eingriffsschwelle also in das Gefahrenvorfeld. Wie weit diese Vorverlagerung erfolgen darf, wird aber nicht geregelt. Das Tatbestandsmerkmal „tatsächliche“ grenzt die „vorhersehbare Gefahr“ nicht ein. Es trifft keine Aussage in Bezug auf die Anforderungen, die an die Qualität der Prognose, den Zeithorizont oder den Wahrscheinlichkeitsgrad zu stellen sind.

Die Norm enthält zwar das einschränkende Tatbestandsmerkmal, wonach die Suche „auf diese Weise unbedingt erforderlich" sein muss. Dieses Merkmal ist jedoch nicht geeignet, die fehlende tatbestandliche Bestimmtheit hinsichtlich der Gefahrenschwelle zu kompensieren. Es adressiert lediglich die Zweck-Mittel-Relation, nicht aber das Gewicht des Anlasses. Das Merkmal sagt also nichts darüber aus, ob die Situation das Ausmaß des Grundrechtseingriffs überhaupt rechtfertigt und ist ohnehin im Rahmen der Verhältnismäßigkeitsprüfung im engeren Sinne zu prüfen. Diese setzt ihrerseits aber eine definierte Eingriffsschwelle als Ausgangspunkt benötigt.

v. Einsatz nicht lediglich zum Schutz besonders gewichtiger Rechtsgüter

§ 14 Abs. 9 Satz 2 HSOG erlaubt auch den Einsatz der biometrischen Echtzeit-Fernidentifizierung zum Schutz von Rechtsgütern, die nicht das nach den oben aufgeführten verfassungsrechtlichen Maßstäben erforderliche Gewicht aufweisen.

Das Bundesverfassungsgericht hat die Anforderung aufgestellt, dass in Fällen, in denen der Gesetzgeber das zu schützende Rechtsgut nicht unmittelbar benennt, sondern an Straftatbestände anknüpft, diese entsprechend schwer wiegen müssen,

> BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19, BeckRS 2025, 19412, Rn. 137.

Zur erforderlichen Schwere der Straftaten führt es aus:

> *„Dem verfassungsrechtlichen Erfordernis eines besonders gewichtigen Rechtsguts entspricht jedenfalls eine Begrenzung auf **besonders schwere Straftaten** im verfassungsrechtlichen Sinn, also zunächst solche, die mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht sind (vgl. auch BVerfGE 165, 1 <93 Rn. 179>; näher BVerfGE 169, 130 <219 Rn. 203> jeweils*

m.w.N.). Grundsätzlich kann aber auch eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren als besonders schwer eingestuft werden, wenn dies nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar erscheint (näher dazu BVerfGE 169, 130 <219 f. Rn. 205>) [Hervorhebungen durch Unterzeichner],

BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19, BeckRS 2025, 19412, Rn. 137.

§ 14 Abs. 9 S. 2 HSOG nennt als Anknüpfungspunkt die Opfereigenschaft bestimmter Straftaten, etwa nach §§ 232, 176 oder 184c StGB. Die mit der Maßnahme zu schützenden Rechtsgüter werden nicht benannt; es wird – zumindest mittelbar – an bestimmte Straftaten angeknüpft. Bereits insoweit bestehen aber – wie oben ausgeführt (aa) – mit dem Bestimmtheitsgebot unvereinbare Unklarheiten darüber, welche konkreten Tatbestände und Fallgestaltungen erfasst sein sollen. Unabhängig davon gewährleistet die bloße Opfereigenschaft hinsichtlich dieser „Straftaten“ jedoch nicht in jedem Fall eine gegenwärtige oder zumindest konkretisierte Gefährdung von Rechtsgütern von besonders hohem Gewicht wie Leib, Leben oder persönlicher Freiheit.

Zum einen erfasst der Tatbestand auch Fälle, die dem Schutz von anderen, als den zuvor benannten Rechtsgütern dienen soll. So schützt § 232 Abs. 1 S. 1 Nr. 1 b) StGB etwa auch die persönliche Freiheit, über die Arbeitskraft zu verfügen,

Eisele, in: Tübinger Kommentar StGB, 2025, § 232 Rn. 9.

Diese Schutzrichtung verdeutlicht, dass nicht jede Tatbestandsverwirklichung zwangsläufig mit einer konkreten Gefährdung von Leib, Leben oder der körperlichen Fortbewegungsfreiheit einhergeht. Gleiches gilt für Konstellationen des § 232 Abs. 1 Satz 1 Nr. 1 lit. b) und d) StGB, etwa wenn eine Person zur Begehung von Vermögensdelikten wie Ladendiebstählen ausgebeutet werden soll. Die Opfer von Taten nach § 232 StGB werden zwar auf verwerfliche Weise ausgenutzt und in ihrer Handlungsfreiheit beschränkt, eine konkrete Gefährdung besonders gewichtiger Rechtsgüter wie Leib, Leben oder Freiheit der Person geht damit aber nicht in jedem Fall einher.

Auch bei Straftaten nach §§ 184b und 184c StGB - – die nach Definition der Lanzarote-Konvention des Europarates unter sexuelle Ausbeutung fallen (siehe dazu oben bb)(2)(2)) – ist nach Schutzrichtung und Begehungsform zu differenzieren. Die diesen Normen zugrunde liegende sexuelle Ausbeutung kann gravierende psychische und physische Folgen für die betroffenen Kinder und Jugendlichen haben. Die Strafbarkeit des Verbreitens, Erwerbens oder Besitzes entsprechender Darstellungen dient daher nicht nur dem individuellen Opferschutz, sondern auch der Bekämpfung des Marktes für entsprechende Inhalte.

Darüber hinaus erlaubt die Rechtsgrundlage eine Anknüpfung an Straftaten, die nicht als besonders schwer einzustufen sind. Wie bereits ausgeführt, können aufgrund der unzureichenden Spezifizierung des Begriffs „sexuelle Ausbeutung“ auch Straftaten wie die Ausbeutung von Prostituierten (§ 180a StGB), die Förderung sexueller Handlungen Minderjähriger (§ 180 StGB), die Verbreitung, der Erwerb und Besitz jugendpornographischer Inhalte (§ 184c) und die (versuchte) Nötigung (§ 240 StGB) darunter fallen (siehe dazu oben bb)(2)(a)). Diese sind jedoch mit einem Höchststrafrahmen von 3 Jahren in den Bereich der leichten Kriminalität zu verorten. Damit wird der Anwendungsbereich der Maßnahme auf Fälle ausgeweitet, in denen der Einsatz aufgrund des hohen Eingriffsgewichts unverhältnismäßig ist.

Schließlich enthält § 14 Abs. 9 S. 2 HSOG keine Normierung der Rechtsgüter, zu deren Schutz die Suche nach vermissten Personen mittels biometrischer Echtzeit-Fernidentifizierung zulässig sein soll. Anders als bei der Suche nach Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung, bei der sich zumindest mittelbar aus der Anknüpfung an bestimmte Straftaten ein Bezug zu Rechtsgütern wie Leib, Leben oder persönlicher Freiheit herstellen lässt, fehlt bei der Ermächtigung zur Suche nach vermissten Personen jede normative Eingrenzung auf bestimmte zu schützende Rechtsgüter.

Die sehr weiten Tatbestandsvoraussetzung lassen insoweit einen Einsatz der biometrischen-Echtzeitidentifizierung auch in Fällen zu, in denen keine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut der vermissten Person besteht und die Maßnahme dadurch nicht einem solchen Rechtsgutsschutz dient. Wie bereits ausgeführt, könnten Konstellationen darunter fallen, in denen etwa die Person ohne bestehende Gefahrenlage aus eigenem Antrieb untergetaucht ist oder sich in der Obhut des anderen Elternteils befindet

(siehe dazu oben bb)(2)(b)). Ohne eine gesetzliche Eingrenzung auf Fälle, in denen eine zumindest konkretisierte Gefahr für besonders gewichtige Rechtsgüter besteht, ist eine auf § 14 Abs. 9 S. 2 HSOG gestützte Maßnahme unverhältnismäßig.

Die Auffassung des Beklagten, die gezielte Suche nach vermissten Minderjährigen diene in jedem Fall der Abwehr von Gefahren für Leib, Leben, Freiheit und die Menschenwürde vor Missbrauch und Ausbeutung sexueller Art (Klageerwiderung vom 17. Dezember 2025, S. 6), ist aufgrund ihrer Pauschalität als unzutreffend zurückzuweisen. Entsprechendes gilt für die Datenschutzfolgenabschätzung, die die generelle Annahme aufstellt, bei vermissten Minderjährigen sei „mit Blick auf ihre körperliche und intellektuelle Unterlegenheit und die daraus resultierende Schutzbedürftigkeit generell von einer konkreten Gefahrenlage für Leib, Leben, persönliche Freiheit und die ungestörte sexuelle Entwicklung durch physische und psychische Misshandlung, sexuelle Ausbeutung und Entführung auszugehen",

vgl. DSFA, Anlage B7, S. 33.

Diese Annahme ist — wie das Bundeskriminalamt auf seiner Website ausführt — empirisch nicht haltbar (dazu oben bb)(2)(b)). Eine pauschale, auf allgemeinen Erfahrungssätzen gestützte Gefahrenvermutung ersetzt keine konkrete Gefahrenprognose und genügt den verfassungsrechtlichen Anforderungen an die tatbestandliche Eingriffsschwelle nicht.

Hinzu kommt, dass der Beklagte mit dieser Annahme die beiden tatbestandlich eigenständigen Kategorien des § 14 Abs. 9 S. 2 HSOG vermengt. Die Argumentation des Beklagten läuft darauf hinaus, die fehlende Eingriffsschwelle bei der Vermisstenkategorie durch eine pauschale Gleichsetzung mit der Opferkategorie zu kompensieren — was weder dem Gesetzeswortlaut noch den verfassungsrechtlichen Anforderungen entspricht.

vi. Mangelhafte Verfahrensregelungen

Die Regelung des § 14 Abs. 9 – 11 HSOG ist schließlich auch unverhältnismäßig im engeren Sinne, da sie den verfassungsrechtlichen Verfahrensanforderungen nicht genügt. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts sind bei heimlichen eingriffsintensiven Überwachungsmaßnahmen gesetzliche Regelungen zur Wahrung und Herstellung von

Transparenz, individuellem Rechtsschutz und aufsichtlicher Kontrolle erforderlich, um dem Verhältnismäßigkeitsgrundsatz zu genügen,

> BVerfGE 133, 277 (365); BVerfGE 100, 313, (361, 364); BVerfGE 125, 260 (334ff.).

Die Anforderungen ergeben sich aus dem jeweiligen Grundrecht i.V.m. Art 19 Abs. 4 GG,

> BVerfGE 125, 260 (335).

Durch normierte Anforderungen zur Transparenz soll der Umgang mit Daten in einen demokratischen Diskurs eingebunden bleiben. Zudem dienen Transparenzerfordernisse dazu, dass Vertrauen und Rechtssicherheit entstehen können,

> BVerfGE 133, 277 (366).

Auch soll auf diese Weise subjektiver Rechtsschutz für die Betroffenen einer polizeirechtlichen Maßnahme möglich werden und einer diffusen Bedrohlichkeit geheimer staatlicher Beobachtung entgegengewirkt werden,

> BVerfGE 125, 260 (335).

In Konsequenz erhalten Anforderungen an eine wirksame aufsichtliche Kontrolle und an die Transparenz des Behördenhandelns größere Bedeutung, je weniger die Gewährleistung subjektiven Rechtsschutzes möglich ist, etwa, weil es sich um heimliche Maßnahmen handelt,

> BVerfGE 133, 277 (366f.); BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09 und 1 BvR 1140/09 -, NJW 2016, 1781 (1788 Rn. 140).

Zu den Anforderungen an die verhältnismäßige Ausgestaltung von heimlichen Überwachungsmaßnahmen gehören die gesetzliche Anordnung von Benachrichtigungspflichten, Auskunftsrechten, zumutbarem gerichtlichen Rechtsschutz, Sanktionen bei Rechtsverletzungen, einer wirksamen aufsichtlichen Kontrolle und Berichtspflichten,

BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09 und 1 BvR 1140/09 -, NJW 2016, 1781 (1788ff Rn. 136ff.).

Im vorliegenden Fall ist die vorgesehene aufsichtliche Kontrolle mangelhaft. Auch fehlen gesetzlich festgelegte Berichtspflichten, was im Ergebnis zur Unverhältnismäßigkeit und somit Verfassungswidrigkeit der Norm führt.

Zu den Anforderungen an die aufsichtliche Kontrolle führt das BVerfG wie folgt aus:

> „*Insbesondere einer sachgerechten Ausgestaltung der Kontrolle kommt große Bedeutung zu. Diese kann angesichts der möglicherweise hohen Zahl von Maßnahmen etwa nach einem abgestuften Kontrollkonzept zwischen unabhängigen und behördlichen Datenschutzbeauftragten aufgeteilt und auch als stichprobenartiges Vorgehen geregelt werden. Für eine effektive Kontrolle unerlässlich ist dabei, dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden. Wird Software eingesetzt, die komplexere Formen des automatisierten Abgleichs von Daten erlaubt, sind auch Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit erforderlich, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann*“,
>
> BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1206 Rn. 109).

Darüber hinaus setze die Gewährleistung einer wirksamen aufsichtlichen Kontrolle

> *„eine mit wirksamen Befugnissen ausgestattete Stelle – wie nach geltendem Recht die Bundesdatenschutzbeauftragte – voraus (vgl. grundlegend BVerfGE 65, 1 [46] = NJW 1984, 419). Dazu ist erforderlich, dass die Datenerhebungen vollständig protokolliert werden. Es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten der Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält (BVerfGE 133, 277 [370] = NJW 2013, 1499 Rn. 215). Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in ange-*

> *messenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen. Dies ist bei der Ausstattung der Aufsichtsinstanz zu berücksichtigen (vgl. BVerfGE 133, 277 [370 f.] = NJW 2013, 1499 Rn. 217),*
>
> BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09 und 1 BvR 1140/09 -, NJW 2016, 1781 (1788 Rn. 141).

Hinsichtlich der Berichtspflichten stellt das BVerfG folgende Maßstäbe auf:

> *„Da sich die Durchführung von heimlichen Überwachungsmaßnahmen der Wahrnehmung der Betroffenen und der Öffentlichkeit entzieht und dem auch Benachrichtigungspflichten oder Auskunftsrechte mit der Möglichkeit anschließenden subjektiven Rechtsschutzes nur begrenzt entgegenwirken können, sind hinsichtlich der Wahrnehmung dieser Befugnisse regelmäßige Berichte [...] gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen. Sie sind erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Datenerhebung, einschließlich der Handhabung der Benachrichtigungspflichten und Löschungspflichten, zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen (vgl. BVerfGE 133, 277 [372] = NJW 2013, 1499 Rn. 221f.)“,*
>
> BVerfG, Urteil vom 20.04.2016 - 1 BvR 966/09 und 1 BvR 1140/09 -, NJW 2016, 1781 (1788 Rn. 143).

Die gesetzlichen Regelungen zu aufsichtlicher Kontrolle und Berichtspflichten im hessischen Landesrecht genügen diesen Anforderungen nicht vollständig. Hinsichtlich der aufsichtlichen Kontrolle sind sie teilweise erfüllt. § 14 Abs. 10 HSOG normiert zwar umfassende Protokollierungspflichten für die Durchführung der biometrischen Echtzeit-Fernidentifizierung, die auch Begründungspflichten beinhalten. Nach den Vorschriften des hessischen Datenschutz- und Informationsfreiheitsgesetzes ist auch die Kontrolle durch die oder den hessischen Datenschutzbeauftragte*n eröffnet. Gemäß Nr. 4 der Verwaltungsvorschriften zu § 14 Abs. 10 S. 3 HSOG ist auch jede Verwendung der biometrischen Echtzeit-Fernidentifizierung der oder dem hessischen Datenschutzbeauftragten mitzuteilen,

vgl. Verwaltungsvorschrift zum notwendigen Inhalt der Begründung nach § 14 Abs. 10 Satz 3 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung, abrufbar unter https://www.rv.hessenrecht.hessen.de/bshe/document/VVHE-VVHE000021064 (Letzter Abruf: 31.12.2025)

Allerdings gibt es keinerlei gesetzliche Vorgabe zu turnusmäßigen Pflichtkontrollen, deren Abstand ein gewisses Höchstmaß nicht überschreiten darf, was unter Berücksichtigung der Intensität des Eingriffs, der Heimlichkeit und der damit einhergehenden geringeren Kontrollmöglichkeiten durch Betroffene geboten ist.

Gesetzlich normierte Berichtspflichten über nach § 14 Abs. 9 – 11 HSOG durchgeführte Maßnahmen gegenüber Parlament und Öffentlichkeit fehlen darüber hinaus gänzlich. Die in § 17a HSOG aufgeführten Berichtspflichten beziehen sich nur auf Maßnahmen nach den §§ 15 – 17 HSOG. Auch in anderen hessischen Landesgesetzen sind keine entsprechenden Berichtspflichten vorhanden.

Darüber hinaus fehlt es auch an normierten Pflichten zur Löschung für die gewonnenen Daten. Zur Wahrung des Verhältnismäßigkeitsgrundsatzes sind als verfahrensrechtliche Schutzvorkehrungen neben Aufklärungs- und Auskunftspflichten jedoch auch Löschungspflichten wesentlich,

BVerfG, Urteil v. 15.12.1983 – 1 BvR 209/83 -, NJW 1984, 419 (422).

Bereits im Falle der automatisierten Kennzeichenerkennung, die ebenfalls eine automatisierte Datenanalyse – jedoch mit weit weniger sensiblen Daten – vorsieht, hat das BVerfG verlangt, dass die gesetzliche Grundlage tragfähige Regelungen zur Datennutzung und -löschung vorsehen muss, um den Verhältnismäßigkeitsanforderungen zu genügen,

BVerfG, Beschluss vom 18.12.2018 – 1 BvR 142/15 -, NJW 2019, 827 (833f Rn 90).

Nach Angaben des Beklagten werden die erhobenen Daten sofort gelöscht, wenn der eingestellte Mindestähnlichkeitswert in Bezug auf das Referenzbildmaterial nicht erreicht wird und damit ein sog. „Nicht-Treffer“ vorliegt (Klageerwiderung vom 17. Dezember 2025, S. 9). Diese Löschung erfolge durch einen automatisch ausgelösten Prozess gewöhnlich innerhalb

von wenigen Sekunden nach dem Datenabgleich und sei irreversibel. Zwar mag die eingesetztes Software tatsächlich auf diese Weise funktionieren. Normierte Löschpflichten sieht die gesetzliche Grundlage jedoch nicht vor. § 14 Abs. 9 – 11 HSG erlaubt damit grundsätzlich auch den Einsatz einer Software, die die erhobenen Daten nicht direkt löscht.

Zudem fehlen gesetzliche Speicher- und Löschpflichten für die im Trefferfall erhobenen Daten. Nach Angaben des Beklagten werden alle Treffermeldungen mit dem vom VAS Videmo360 erkannten Bild der erfassten Person gespeichert (Klageerwiderung vom 17. Dezember 2025, S. 9). Dies gilt für sämtliche Personen, die den von den zuständigen Polizeibeamt:innen bei jedem Einsatz selbst festzulegenden Mindestähnlichkeitswert überschreiten,

vgl. DSFA, Anlage B7, S. 9.

Wie bereits ausgeführt, kann abhängig von der Festlegung dieser Schwelle die Anzahl der Treffer und damit die gespeicherten Personen und ihre biometrischen Daten stark variieren (dazu oben unter bb)(2)(c)).

Die Datenschutzfolgenabschätzung beschreibt darüber hinaus, dass bestätigte Treffermeldungen einer Plausibilitätskontrolle durch die Vollzugskräfte im VOC unterzogen werden und anschließend für die Dauer der laufenden Suchmaßnahme als operativer Rückhalt gespeichert bleiben, damit sie bei weiteren Treffermeldungen als Hilfsmittel für die Plausibilitätskontrolle herangezogen werden können. Zudem erhalten die Fachdienststellen einen Export des jeweiligen Trefferbildes für die Fallbearbeitung und die Ablage in der Kriminalakte. Nach Verfahrensabschluss werden die Identitäten laut den Ausführungen in der Datenschutzfolgenabschätzung gelöscht,

vgl. DSFA, Anlage B7, S. 23.

Es ist jedoch weder gesetzlich vorgeschrieben, dass eine Plausibilitätskontrolle überhaupt durchzuführen ist, noch nach welchen Kriterien und in welchem Verfahren sie zu erfolgen hat. Auch enthält § 14 Abs. 9–11 HSOG weder Vorgaben dazu, wie lange die Daten von als Treffer erfassten Personen gespeichert werden dürfen, noch ab welchem Zeitpunkt eine Löschung zu erfolgen hat — weder für Personen, die zutreffend als gesuchte Person identifi-

ziert wurden, noch für Personen, die fälschlicherweise als Treffer angezeigt wurden und für die Maßnahme keinen Anlass gegeben haben. Gerade für letztere ist das Fehlen einer normierten Löschpflicht besonders gravierend, da sie durch die längerfristige Speicherung ihrer biometrischen Daten einem Eingriff ausgesetzt sind, der außer Verhältnis zum Umstand steht, dass sie lediglich zufällig in das Sichtfeld einer Überwachungskamera geraten sind.

Darüber hinaus enthält die konkret eingesetzte Software VAS Videmo360 ausweislich der Datenschutzfolgenabschätzung eine Suchfunktion, die eine nachträgliche biometrische Fernidentifizierung (sog. retrograde Suche) von Personen in einem abgeschlossenen Datenbestand ermöglicht. Dort führt das Polizeipräsidium am Main zwar aus, dass diese Funktion bei der Echtzeit-Fernidentifizierung keine Anwendung finde,

> vgl. DSFA, Anlage B7, S. 12.

§ 14 Abs. 9–11 HSOG enthält jedoch keine gesetzlichen Vorgaben, die eine missbräuchliche Nutzung dieser Funktion ausschließen. Es fehlen insbesondere normierte Pflichten, wonach die retrograde Suchfunktion beim Einsatz der Echtzeit-Fernidentifizierung dauerhaft und ohne eigenständige Wiederherstellungsmöglichkeit durch die handelnde Polizeibehörde zu deaktivieren ist, sowie konkrete organisatorische und technische Vorgaben, die eine Aktivierung dieser Funktion verhindern. Allein der Umstand, dass die Polizeibehörde nach eigenen Angaben von dieser Funktion keinen Gebrauch macht, genügt den verfassungsrechtlichen Anforderungen nicht. Das Gebot der Normenbestimmtheit und Normenklarheit verlangt, dass die Grenzen einer Ermächtigungsgrundlage durch den Gesetzgeber selbst verbindlich gezogen werden und nicht durch eine freiwillige Selbstbeschränkung der handelnden Behörde, die jederzeit geändert werden kann.

Auch fehlen gesetzliche Benachrichtigungspflichten. Das Bundesverfassungsgericht hat zu besonders eingriffsintensiven geheimen Überwachungsmaßnahmen den Maßstab aufgestellt, dass zu den Anforderungen an die verhältnismäßige Ausgestaltung dieser

> *„die gesetzliche Anordnung von Benachrichtigungspflichten [gehören]. Da solche Maßnahmen, um ihren Zweck zu erreichen, heimlich durchgeführt werden müssen, hat der Gesetzgeber zur Gewährleistung subjektiven Rechtsschutzes iSd Art. 19 IV GG vorzusehen, dass die Betroffenen zumindest nach-*

> *träglich von den Überwachungsmaßnahmen grundsätzlich in Kenntnis zu setzen sind“,*
>
> BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 (1788 Rn. 136).

Zumindest in Fällen, in denen eine Person auf Grundlage der biometrischen Echtzeit-Fernidentifizierung von polizeilichen Anschlussmaßnahmen betroffen ist, muss die Rechtsgrundlage eine Benachrichtigungspflicht enthalten, damit die betroffene Person wirksam nachträglich Rechtsschutz ersuchen kann.

Schließlich macht auch die Automatisierung des Datenabgleichs spezifische Verfahrensregelungen erforderlich, die im HSOG bisher nicht geregelt sind. Zur Echtzeit-Fernidentifizierung wird eine Software eingesetzt, die komplexere Formen des automatisierten Abgleichs von Daten erlaubt. Damit geht eine spezifische Fehleranfälligkeit einher. Ist eine Software etwa unerkannt fehlerhaft, kann das zu falschen Treffern und damit verbunden gefahrenabwehrrechtlichen Folgemaßnahmen und weiteren Grundrechtseingriffen führen. Das BVerfG hat deshalb anerkannt, dass der Gesetzgeber aufgefordert sein kann, ein staatliches Monitoring der Entwicklung der eingesetzten Software zu normieren,

> BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19 und 1 BvR 2634/20 -, NJW 2023, 1196 (1206 Rn. 109).

Solche Regelungen fehlen in § 14 Abs. 9 - 11 HSOG vollständig. Insbesondere sind weder Vorgaben zu den Anforderungen an die Qualität und Repräsentativität der Trainingsdaten normiert, noch bestehen gesetzliche Pflichten zur regelmäßigen Überprüfung der eingesetzten Software auf Systemfehler und diskriminierende Verzerrungen. Dies ist auch deshalb besonders bedeutsam, da die Fehlerquote der Gesichtserkennung nicht gleichmäßig über alle Bevölkerungsgruppen verteilt ist und insbesondere Persons of Colour, Frauen, Kinder und ältere Menschen überproportional betrifft (siehe dazu oben a)aa)(5)). Die Notwendigkeit solcher gesetzlicher Schutz- und Verfahrensvorkehrungen wird zudem durch die Ausführungen in der Datenschutzfolgenabschätzung untermauert, dass die „Erzeugung der Gesichtstemplates [...] durch ein KI-Modell [erfolgt], dessen genaue Spezifikationen nur dem Hersteller des VAS bekannt ist“ – aber nicht der das System nutzenden Polizeibehörde,

vgl. DSFA, Anlage B7, S. 12.

Dadurch hat die Polizeibehörde weder die Möglichkeit noch das notwendige technische Wissen, um systembedingte Fehler und potentiell diskriminierende Ausgaben zu erkennen und zu beseitigen. Das Fehlen eines gesetzlich vorgeschriebenen Softwaremonitorings ist damit nicht nur ein verfahrensrechtliches Defizit, sondern berührt auch das Diskriminierungsverbot des Art. 3 GG. § 14 Abs. 9 - 11 HSOG genügt damit auch insoweit den verfassungsrechtlichen Verfahrensanforderungen nicht.

b) Unverhältnismäßigkeit im Einzelfall

Die Maßnahme ist auch im Einzelfall unverhältnismäßig.

aa) Legitimer Zweck

Die Maßnahme verfolgt wie oben dargelegt einen legitimen Zweck.

bb) Geeignetheit

Die Maßnahme ist auch dazu geeignet den legitimen Zweck zumindest zu fördern.

cc) Erforderlichkeit

Die Maßnahme ist aus denselben Gründen, die bereits im Rahmen der abstrakten Verhältnismäßigkeitsprüfung dargelegt wurden, auch im Einzelfall nicht in vollem Umfang erforderlich (dazu oben a)cc)(3)). Insbesondere gilt dies für den konkreten Einsatz der Kamera, deren Sichtfeld den Eingangsbereich der Beratungsstelle des Vereins Doña Carmen e.V. erfasst. Für die dort typischerweise in Betracht kommenden Einsatzszenarien – namentlich die Suche nach Opfern von Entführung, Menschenhandel und sexueller Ausbeutung sowie vermissten Personen nach § 14 Abs. 9 S. 2 HSOG – stünden insbesondere mit der Mobilfunkortung mildere, gleich wirksame Mittel zur Verfügung, die eine anlasslose biometrische Erfassung der Kläger:innen und der Klient:innen der Beratungsstelle vermeiden würden.

dd)Angemessenheit

Die Maßnahme ist auch im Einzelfall unangemessen und verletzt die Kläger:innen in ihrem Grundrecht auf informationelle Selbstbestimmung und Vereinigungsfreiheit. Wie bereits oben dargelegt wurde, sind an die Verhältnismäßigkeit von Maßnahmen der Gefahrenabwehr, die mit besonders hoher Intensität in das Grundrecht auf informationelle Selbstbestimmung eingreifen, besonders hohe Anforderungen zu stellen. Diese Anforderungen sind auch im konkreten Fall nicht erfüllt.

(1) Besonders hohes Eingriffsgewicht im konkreten Fall

Das bereits zuvor im Abstrakten ausgeführte besonders hohe Eingriffsgewicht von Maßnahmen nach § 14 Abs. 9 – 11 HSOG (siehe dazu oben 2.a)aa)), gilt in gleicher Weise für den konkret gegenüber den Kläger:innen durchgeführten und zukünftig drohenden Einsatz der biometrischen Echtzeit-Fernidentifizierung.

Dabei wirkt sich eingriffsverstärkend aus, dass im vorliegenden Fall die Kläger:innen sowohl als Privatpersonen als auch in ihrer Eigenschaft als Vorstandsmitglieder der Beratungsstelle von der biometrischen Erfassung betroffen sind. Die damit einhergehenden Abschreckungs- und Einschüchterungseffekte beeinträchtigen nicht nur ihr persönliches Verhalten im öffentlichen Raum, sondern darüber hinaus in erheblicher Weise die von Art. 9 Abs. 1 GG geschützte Durchführung von Vereinstätigkeiten und gefährden dadurch die Funktionsfähigkeit der Beratungsstelle. Zudem können sich die Kläger:innen der Maßnahme nicht entziehen, ohne ihre vereinsbezogene Tätigkeit vollständig aufzugeben. Als Vorstandsmitglieder des Vereins Doña Carmen e.V. sind sie verpflichtet, die Vereinsräumlichkeiten regelmäßig aufzusuchen, sei es für [redacted] oder die Wahrnehmung sonstiger Vorstandsaufgaben. Diese Tätigkeiten führen sie zwangsläufig in das Sichtfeld der Kamera, ohne dass sie hierauf Einfluss nehmen könnten. Anders als zufällig vorbeilaufende Passanten, die den erfassten Bereich meiden könnten, sind die Kläger:innen dauerhaft und ohne Ausweichmöglichkeit der biometrischen Erfassung ausgesetzt.

Die hohe Wahrscheinlichkeit einer tatsächlichen Betroffenheit der Kläger:innen wird durch die bisherige Einsatzpraxis des Beklagten untermauert. Nach den eigenen Angaben des Be-

klagten wurden im Zeitraum vom 10. Juli 2025 bis zum 28. Februar 2026 acht Maßnahmen nach § 14 Abs. 9 HSOG durchgeführt, die jeweils nach den Angaben in der Datenschutzfolgenabschätzung einen Zeitraum von bis zu drei Monaten umfassen können,

vgl. DSFA, Anlage B7, S. 43.

Da die Kläger:innen die Vereinsräumlichkeiten wöchentlich [redacted] aufsuchen und dabei zwangsläufig das Sichtfeld der Kamera durchqueren, ist mit hoher Wahrscheinlichkeit davon auszugehen, dass sie bereits im Rahmen vergangener Maßnahmen biometrisch erfasst wurden und zukünftig weiter erfasst werden. Da die Maßnahme heimlich durchgeführt wird und keine Benachrichtigungspflichten bestehen, sind sie faktisch in ihren Rechtsschutzmöglichkeiten eingeschränkt, was das konkrete Eingriffsgewicht weiter erhöht.

Hinzu kommen die erheblichen chilling effects auf die Klient:innen der Beratungsstelle. Die streitgegenständliche Kamera erfasst den Eingang der Beratungsstelle, d.h. genau den Ort, an dem Personen erscheinen, die vertraulich und niedrigeschwellig Bera-tungsangebote des Vereins in Anspruch nehmen möchten. Die Beratungsstelle ist an [redacted] die Woche geöffnet und bietet neben persönlicher Beratung auch Krisenintervention vor Ort, Dolmetscherleistungen bei Behördengängen sowie Langzeit-Einzelfallbetreuung in Fällen mit komplexer Problematik an. Der Verein tritt insbesondere für Anliegen von migrantischen Sexarbeiter*innen ein und unterstützt sie vor Ort mit sozialer Beratung. Er hat über Jahrzehnte hinweg mit erheblichem ehrenamtlichem Engagement an einem vertrauensvollen Verhältnis zu den von ihm beratenen Menschen gearbeitet, das die Grundlage seiner gesamten Tätigkeit bildet.

Die Inanspruchnahme eines solchen Beratungsangebots ist für viele Sexarbeiter:innen mit dem Wunsch nach Diskretion und dem Schutz vor sozialer Stigmatisierung verbunden. Gerade in diesem Berufsfeld sind viele Menschen tätig, die vulnerablen Gruppen zugehörig sind und sich vor einer umfassenden staatlichen Überwachung sowie damit einhergehenden Diskriminierungs- und Stigmatisierungseffekten fürchten. Die Überwachung des Eingangsbereichs und die damit verbundene Möglichkeit, nachzuvollziehen, wer die Räumlichkeiten betritt und verlässt, kann auf potenzielle Klient:innen eine erhebliche Abschreckungswirkung entfalten und dazu führen, dass sie auf die Inanspruchnahme der Beratungsleistungen ver-

zichten – mit der Folge, dass sie im Falle gesundheitlicher Probleme, sexueller Gewalt oder psychischer Belastungen den Zu-gang zu einer seit vielen Jahren vertrauten Anlaufstelle verlieren und in akuten Krisensituationen ohne Unterstützung bleiben, was zu einer Gefährdung ihrer physischen sowie psychischen Gesundheit führt. Diese im konkreten Fall drohenden Schäden gehen weit über die in der Datenschutzfolgenabschätzung benannten Gefahren – „Verlust an Lebensqualität durch Abschreckung vom Betreten von Videoschutzzonen“ und „Stress durch das Gefühl des Überwacht-Werdens in den Videoschutzzonen“ (vgl. DSFA, Anlage B7, S. 80) – hinaus.

Damit gefährdet die Maßnahme nach § 14 Abs. 9 – 11 HSOG neben der Freiheit der Kläger:innen, sich ohne Überwachungsdruck im öffentlichen Raum zu bewegen und ihr Verhalten unbeeinflusst von staatlicher Beobachtung zu gestalten, auch in erheblicher Weise den Vereinszweck und zentrale Vereinstätigkeiten sowie mittelbar das physische und psychische Wohlbefinden der auf die Beratungsstelle angewiesenen Sexarbeiter:innen.

Soweit der Beklagte aus der Anzahl der Beschlussanträge und durchgeführten Maßnahmen auf einen „sensiblen und verantwortungsvollen Umgang mit den gesetzlichen Voraussetzungen des § 14 Abs. 9 HSOG" und eine „restriktive Anwendung" schließt (Schriftsatz vom 16. März 2026, S. 4), vermag dies das Eingriffsgewicht nicht zu mildern. Das Eingriffsgewicht einer staatlichen Maßnahme bestimmt sich nach den bereits angeführten objektiven Kriterien (siehe dazu oben 2.a)aa) und richtet sich nicht nach der subjektiven Zurückhaltung der handelnden Behörde hinsichtlich der Durchführung der Maßnahme.

Darüber hinaus lässt sich aus einem derzeit zurückhaltenden Einsatz nichts über die künftige Einsatzpraxis ableiten. Die gesetzliche Ermächtigungsgrundlage in § 14 Abs. 9 – 11 HSOG erlaubt den Einsatz der biometrischen Echtzeit-Fernidentifizierung in deutlich größerem Umfang, als bisher praktiziert, und bietet dafür keine hinreichend bestimmten und angemessenen gesetzlichen Begrenzungen.

(2) Unangemessenheit

Der besonders hohen Eingriffsintensität stehen im vorliegenden Fall keine hinreichend konkretisierten Gefahrenlagen und kein ausreichend bedeutsamer Rechtsgüterschutz durch

den Einsatz der biometrischen Echtzeit-Fernidentifizierung nach § 14 Abs. 9 – 11 HSOG mithilfe der Kamera, deren Sichtfeld sich auf den Eingangsbereich des Vereins Doña Carmen e.V. erstreckt, gegenüber, die die Maßnahme rechtfertigen könnten. Daher ist die Maßnahme im konkreten Fall unverhältnismäßig im engeren Sinne.

Da der Beklagte die konkrete Grundlage der jeweiligen Einsatzentscheidungen — insbesondere die im Einzelfall zugrunde gelegten Gefahrenlagen und Rechtsgüter — weder offengelegt noch vorgetragen hat, ist den Kläger:innen eine fallspezifische Auseinandersetzung mit den jeweiligen Abwägungsentscheidungen nicht möglich. Aus der Weite der Rechtsgrundlage und der aus der Datenschutzfolgenabschätzung ersichtlichen Einsatzpraxis ergibt sich jedoch, dass § 14 Abs. 9 S. 2 HSOG — wie oben unter der abstrakten Verhältnismäßigkeitsprüfung umfassend ausgeführt (dazu oben a)bb) und cc)(3)) — auch Konstellationen erfasst, in denen keine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut festgestellt werden muss, und dass die Maßnahme in der Praxis auch dann eingesetzt wird, wenn diese Voraussetzung nicht vorliegt. Das gilt im konkreten Fall in besonderem Maße. Der Einsatz der Kamera an der [redacted] erfolgt nach den Angaben des Beklagten insbesondere zur Suche nach vermissten Minderjährigen (Klageerwiderung vom 17. Dezember 2025, S. 4, DSFA, Anlage B7, S. 6 f.). Die Vermissteneigenschaft als solche begründet jedoch keine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut (dazu oben a)cc)(3)(cc)). Ein erheblicher Teil der im polizeilichen Fahndungssystem gespeicherten vermissten Minderjährigen befindet sich nach den Angaben des Bundeskriminalamts in keiner akuten Gefährdungssituation. Für diese Fälle steht das Eingriffsgewicht der Maßnahme außer Verhältnis zum verfolgten Zweck und führt insoweit zur Unverhältnismäßigkeit.

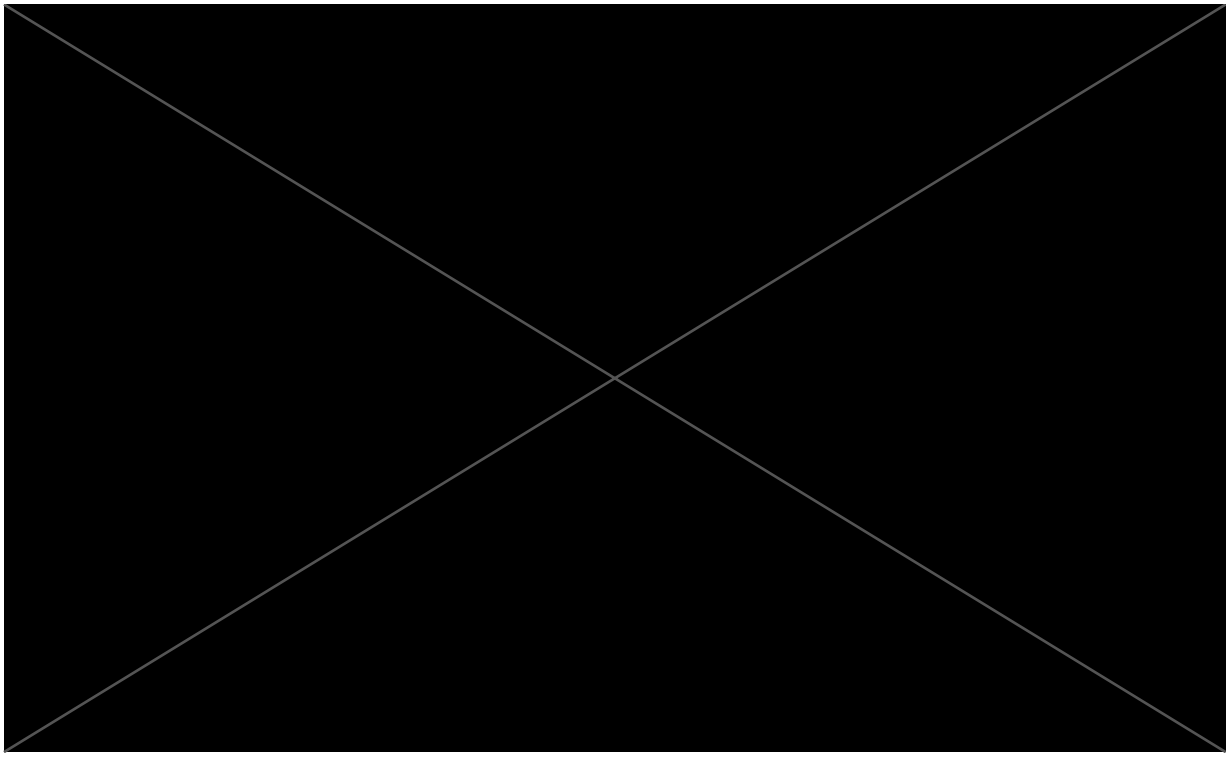
Die Unverhältnismäßigkeit der Maßnahme im Einzelfall ergibt sich auch aus der Auswahl des konkreten Kamerastandorts für den Einsatz der biometrischen Echtzeit-Fernidentifizierung. Es ist weder vorgetragen noch ersichtlich, warum gerade der Eingangsbereich einer Beratungsstelle für Sexarbeiter:innen als Standort für eine Kamera, mit der Maßnahmen nach § 14 Abs. 9 – 11 HSOG durchgeführt werden können, geeignet sein soll, um die in der Rechtsnorm genannten Zwecke zu verwirklichen. Für die Suche nach Terrorismusverdächtigen nach § 14 Abs. 9 S. 1 HSOG fehlen konkrete Anhaltspunkte, weshalb dieser Standort besondere taktische Bedeutung haben sollte. Für die Suche nach vermissten Minderjährigen

nach § 14 Abs. 9 S. 2 HSOG ist die Erfassung des Eingangsbereichs einer Beratungsstelle, die sich ausweislich ihres Satzungszwecks an Erwachsene im Bereich der Sexarbeit richtet, gleichfalls nicht naheliegend.

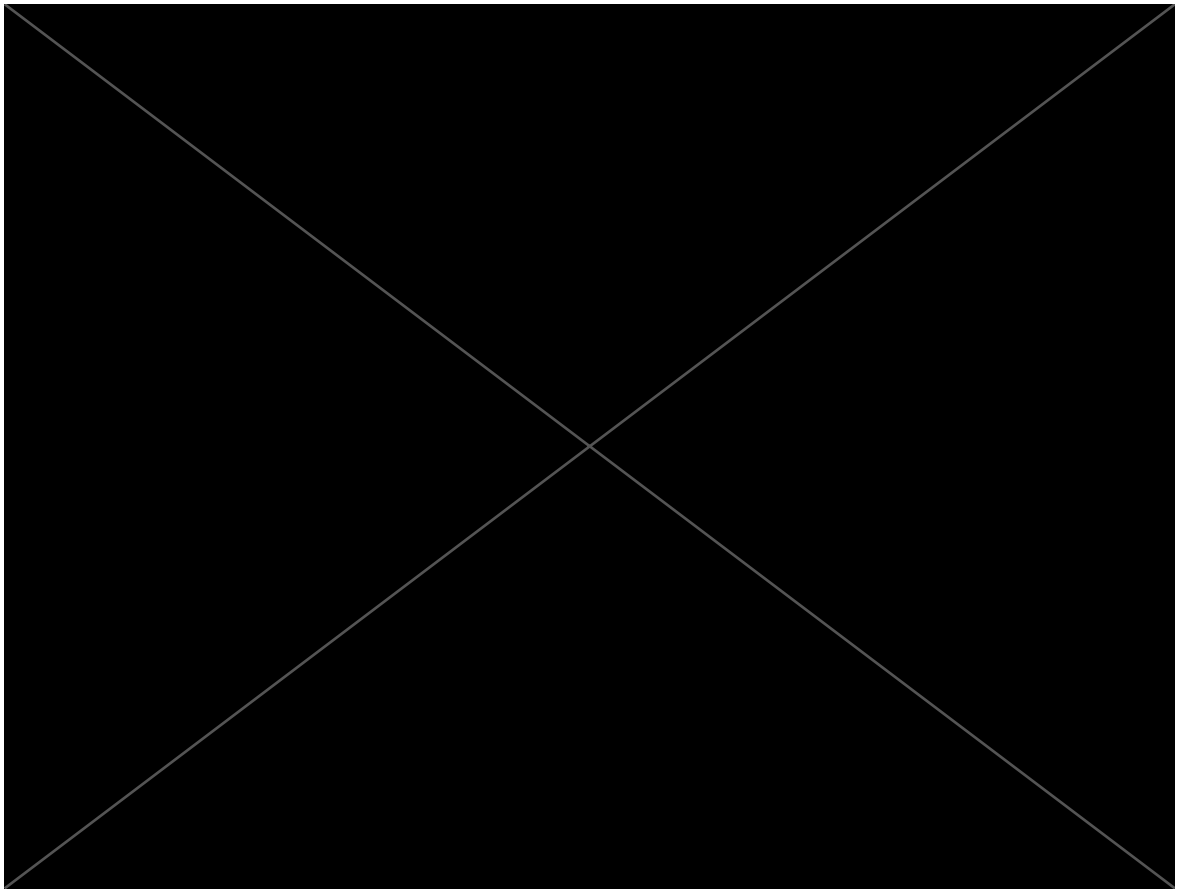
Darüber hinaus steht die Maßnahme im vorliegenden Fall auch außer Verhältnis zum damit einhergehenden besonders schwerwiegenden Eingriff in das Grundrecht auf Vereinigungsfreiheit aus Art. 9 Abs. 1 GG der Kläger:innen. Der Einsatz der biometrischen Echtzeit-Fernidentifizierung am Eingangsbereich der Beratungsstelle beeinträchtigt in erheblicher Weise die Fähigkeit des Vereins Doña Carmen e.V., seinen satzungsgemäßen Zweck — die Unterstützung und Beratung von Sexarbeiter:innen — effektiv zu verfolgen. Dabei sind die Kläger:innen nicht nur als Vorstandsmitglieder in ihren Vereinstätigkeiten beeinträchtigt, sondern die Erreichung des gesamten Vereinszwecks ist gefährdet. Eine Beratungsstelle, die darauf angewiesen ist, dass schutzbedürftige Klient:innen sie niedrigschwellig und ohne Furcht vor staatlicher Überwachung aufsuchen, verliert durch die verdeckte und automatisierte biometrische Erfassung ihres Eingangsbereichs die wesentliche Voraussetzung ihrer Wirksamkeit und Funktionsfähigkeit. Das Polizeipräsidium Frankfurt am Main hat bei der Standortauswahl die vereinsrechtliche Dimension der Maßnahme nicht hinreichend berücksichtigt. Auch die Datenschutzfolgenabschätzung enthält keine Auseinandersetzung mit Art. 9 GG, obwohl der Einsatz unmittelbar am Eingang einer Vereinsberatungsstelle erfolgt. Daher ist die Maßnahme im vorliegenden Fall auch insoweit unverhältnismäßig.

(3) Unzureichende Ausblendung von Privatzonen

Die Ausführungen des Beklagten, dass der Eingangsbereich der Vereinsräumlichkeiten von Doña Carmen e.V. dauerhaft durch technische Maßnahmen ausgeblendet werde (Klageerwiderung vom 17. Dezember 2025, S. 3), ist unzutreffend und vermag die Unverhältnismäßigkeit der Maßnahme nicht zu beseitigen.



Wie das angezeigte Bild des Videoüberwachungssystems (Anlage B5) zeigt, wird durch den schwarzen Balken lediglich eine der Türen in der Häuserfront geschwärzt. Dabei handelt es sich jedoch nicht um den tatsächlichen Eingang zur Beratungsstelle, durch den Ratsuchende die Räumlichkeiten des Vereins betreten. Der eigentliche Eingang – erkennbar an der dort angebrachten Klingel und der Hausnummer – liegt daneben und ist im Videobild vollständig sichtbar. Auch ist fraglich, ob die Schwärzung dieses Bereichs immer angezeigt wird, oder ob diese lediglich bei der Weiterverbreitung des Videomaterials eingefügt wird.



Darüber hinaus zeigt ein Vergleich der vorliegenden Aufnahmen, dass im von der Polizei vorgelegten Foto nicht nur eine Tür geschwärzt, sondern auch ein Teil der Häuserfront offenbar nachträglich herausgeschnitten wurde. Dieser Umstand begründet erhebliche Zweifel an der Verlässlichkeit und Vollständigkeit des vorgelegten Bildmaterials.

Selbst wenn der tatsächliche Eingang der Beratungsstelle ebenfalls geschwärzt würde, wäre dies nicht geeignet, die grundrechtlichen Bedenken auszuräumen. Denn auch bei geschwärztem Hauseingang bleibt auf den Aufnahmen erkennbar, welche Personen sich in welche Richtung bewegen und welche Gebäude sie betreten und verlassen. Wer von rechts oder links kommend in einen geschwärzten Eingangsbereich geht und auf der anderen Seite nicht mehr auftaucht, ist erkennbar in das betreffende Gebäude gegangen und damit als potenzielle:r Klient:in der Beratungsstelle identifizierbar. Weder schwarze Balken noch das Herausschneiden von Teilen der Häuserfront verhindern, dass solche Rückschlüsse gezogen werden können. Gerade in Betracht des oben angeführten chilling effects und der Möglichkeit anhand des Videomaterials Bewegungsprofile zu erstellen, ist diese Schwärzung nicht ausreichend, um solchen Effekten entgegenzuwirken.Der Nachbesserungsversuch des Poli-

zeipräsidiums Frankfurt am Main ist damit unzureichend und vermag eine Verhältnismäßigkeit der Maßnahme nicht zu begründen.

c) Unionsrechtswidrigkeit

Der Einsatz der biometrischen Echtzeit-Fernidentifizierung nach § 14 Abs. 9 - 11 HSOG verstößt gegen Art. 5 Abs. 2 UAbs. 2 S. 2, Abs. 3, Abs. 5 S. 2 und Art. 14 Abs. 5 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (nachfolgend KI-VO) und ist unionsrechtswidrig.

aa) Anwendbarkeit Unionsrecht

Der Anwendungsbereich der KI-VO ist nach Art. 2 Abs. 1 lit. b KI-VO eröffnet, da die Maßnahmen nach § 14 Abs. 9 - 11 HSOG auf der Verwendung eines biometrisches Echtzeit-Fernidentifizierungssystem als ein KI-System i.S.d. Art. 3 Nr. 1, Nr. 42 KI-VO basiert und durch die Polizeibehörde Frankfurt als in der Union ansässigen Betreiber i.S.d. Art. 3 Nr. 4 durchgeführt werden.

bb) Verstoß gegen Art. 5 Abs. 5 S. 2 i.V.m. Abs. 3 KI-VO

Die Maßnahmen nach § 14 Abs. 9 - 11 HSOG verstoßen gegen Art. 5 Abs. 5 S. 2 i.V.m. Abs. 3 KI-VO, da die ihnen zugrunde liegenden Rechtsgrundlagen entgegen der Auffassung der Beklagten (Klageerwiderung vom 17. Dezember 2025, S. 6) keine ausreichenden detaillierten Vorschriften für die Ausübung der in Absatz 3 genannten Genehmigungen enthalten.

Nach Art. 5 Abs. 5 S. 2 KI-VO legen die betreffenden Mitgliedstaaten, die eine Ermächtigungsgrundlage für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme geschaffen haben, in ihrem nationalen Recht unter anderem die erforderlichen detaillierten Vorschriften für die Ausübung der in Absatz 3 genannten Genehmigungen fest. Bei einer solchen Ausübung, d.h. dem konkreten Einsatz des KI-Systems nach erteilter Genehmigung, darf der Betreiber gem. Art. 5 Abs. 3 UAbs. 2 S. 3 KI-VO nicht ausschließlich auf der Grund-

lage der Ausgabe des biometrischen Echtzeit-Fernidentifizierungssystems eine Entscheidung mit einer nachteiligen Rechtsfolge für eine Person treffen.

So darf etwa eine gesuchte Person, deren Standort mit der Maßnahme festgestellt werden konnte, nicht ausschließlich aufgrund der Ausgabe des KI-Systems ohne weitergehende menschliche Überprüfung in Gewahrsam genommen werden. Die Überprüfungen können sich etwa auf die Frage beziehen, ob sich eine bestimmte Person an einem anderen Ort befand oder auch, ob es andere Gründe dafür gibt, dass die Person nicht die gesuchte Person sein kann,

> vgl. Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung) vom 29. Juli 2025, C(2025) 5052, Rn. 406.

Art. 14 Abs. 5 KI-VO, der konkrete Anforderungen an die menschliche Aufsicht bei der Verwendung von biometrischen Fernidentifizierungssystemen enthält, konkretisiert die Vorgaben aus Art. 5 Abs. 3 UAbs. 2 S. 3 KI-VO und legt dessen Ausmaß fest,

> vgl. *Wendehorst*, in: Martini/Wendehorst, KI-VO, 1. Auflage 2024, Art. 5 Rn. 187.

Nach Art. 14 Abs. 5 KI-VO müssen die in Absatz 3 des vorliegenden Artikels genannten Vorkehrungen zur Sicherstellung menschlicher Aufsicht so gestaltet sein, dass der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde. Diese Schutzvorkehrung wird mit den bedeutenden Konsequenzen für Personen im Falle eines falschen Treffers begründet, vgl. ErwG 73 KI-VO.

Diesen unionsrechtlichen Anforderungen genügt § 14 Abs. 9 - 11 HSOG nicht. Entgegen Art. 5 Abs. 5 S. 2 KI-VO enthält sie enthält keine Verfahrensvorschriften, die gewährleisten, dass die Vorgaben aus Art. 5 Abs. 3 UAbs. 2 S. 3 i.V.m. Art. 14 Abs. 5 KI-VO bei jedem Einsatz der biometrischen Echtzeit-Fernidentifizierung eingehalten werden. Dieser Verstoß wird auch nicht durch Regelungen in der Verwaltungsvorschrift zum notwendigen Inhalt der Begrün-

dung nach § 14 Abs. 10 Satz 3 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (nachfolgend VV § 14 Abs. 10 Satz 3 HSOG) kompensiert. Soweit dort unter Abschnitt 1 („Leitgedanken“) festgehalten wird, dass auch bei Maßnahmen nach § 14 Abs. 9 - 11 HSOG immer die Entscheidung eines Menschen tragend ist, handelt es sich lediglich um eine unverbindliche programmatische Aussage ohne Außenwirkung. Diese vermag eine nach den unionsrechtlichen Vorgaben erforderliche hinreichend detaillierte gesetzliche Regelung nicht zu ersetzen.

Dies gilt gleichermaßen für die in der Datenschutzfolgenabschätzung enthaltenen Ausführungen zur menschlichen Kontrolle in der Einsatzpraxis. Dort wird beschrieben, dass die „Tatsachenbewertung, ob eine Person identifiziert worden ist bzw. ob es sich bei einer identifizierten Person um die gesuchte Person handelt“ sowie „die Lagebewertung und die Entscheidung über polizeiliche Folgemaßnahmen“ den mit dem System arbeitenden Angehörigen der hessischen Polizei vorbehalten seien. Die „Treffermeldungen werden von den überwachenden Vollzugskräften im VOC einer Plausibilitätskontrolle unterzogen“,

vgl. DSFA, Anlage B7, S. 9 ff.

Eine rein in der Datenschutzfolgenabschätzung beschriebene Verfahrensweise der menschlichen Kontrolle genügt jedoch nicht den zuvor dargestellten unionsrechtlichen Vorgaben, da es sich bei ihr nach Art. 27 JI-Richtlinie bzw. § 67 BDSG um eine von der für die anschließende Datenverarbeitung verantwortlichen Behörde selbst durchgeführte Risikobewertung ohne Rechtssatzqualität handelt. Darüber hinaus wird auch dort nicht ausdrücklich vorgesehen, dass das jeweilige Identifizierungsergebnis von mindestens zwei natürlichen Personen mit der notwendigen Kompetenz, Ausbildung und Befugnis getrennt überprüft und bestätigt wird.

Gerade im Lichte der Wesentlichkeitstheorie sowie der verfassungsrechtlichen Anforderungen an Normenbestimmtheit und Normenklarheit bedarf es einer formell-gesetzlichen Regelung, die das konkrete Verfahren und Sicherungsmechanismen beim Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme klar, nachvollziehbar und verbindlich vorgibt.

cc) Verstoß gegen Art. 5 Abs. 5 S. 2 i.V.m. Abs. 4 S. 2, Abs. 6 KI-VO

Die Durchführung von Maßnahmen nach § 14 Abs. 9 - 11 HSOG verstößt gegen Art. 5 Abs. 5 S. 2 i.V.m. Abs. 4 S. 2, Abs. 6 KI-VO, da die zugrundeliegende Rechtsgrundlage keine Regelungen bezüglich der Berichterstattung enthält.

Art. 5 Abs. 5 S. 2 KI-VO gibt unter anderem vor, dass eine nationale Ermächtigungsgrundlage detaillierte Vorschriften für die bei einer Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems notwendigen Berichterstattung enthalten muss. Dies umfasst insbesondere die in Art. 5 Abs. 4 und Abs. 6 KI-VO geregelten Vorgaben und Abläufe, deren konkrete Umsetzung der nationale Gesetzgeber gesetzlich zu regeln hat,

> vgl. *Wendehorst*, in: Martini/Wendehorst, KI-VO, 1. Auflage 2024, Art. 5 Rn. 182; *Hilgendorf/Härtlein*, in: Hilgendorf/Härtlein, KI-VO, 1. Auflage 2025, Art. 5 Rn. 98.

Art. 5 Abs. 4 S. 1 KI-VO schreibt vor, dass jede Verwendung an die zuständige Marktüberwachungsbehörde und die nationale Datenschutzbehörde gemäß den in Absatz 5 genannten nationalen Vorschriften mitgeteilt werden muss. Dabei muss nach Art. 5 Abs. 4 S. 2 KI-VO die Mitteilung mindestens die in Absatz 6 genannten Angaben enthalten, d.h. Anzahl der gerichtlichen Anordnungen bzw. nachträglichen Entscheidungen und deren Ergebnis, und darf keine sensiblen operativen Daten enthalten.

Solche detaillierten Vorschriften fehlen entgegen der Auffassung der Beklagten (Klageerwiderung vom 17. Dezember 2025, S. 6) in § 14 Abs. 9 - 11 HSOG. Eine Bestimmung der Mitteilungspflichten allein in Verwaltungsvorschriften, die keine Außenwirkung haben, ist unzureichend. Nr. 4 VV § 14 Abs. 10 Satz 3 HSOG bestimmt, dass jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems ist dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit und, sobald die zuständige Marktüberwachungsbehörde nach Art. 5 Abs. 4 KI-VO benannt ist, auch der zuständigen Marktüberwachungsbehörde mitzuteilen ist. Die unionsrechtlichen Vorgaben werden dabei jedoch nur unvollständig wiedergegeben, da Anforderungen für die in einer Mitteilung zu enthaltenen Mindestangaben nach Art. 5 Abs. 4 S. 2 KI-VO fehlen.

Jedenfalls genügt die bloße Bestimmung der Berichtspflichten in der Verwaltungsvorschrift mangels rechtlicher Außenwirkung nicht den unionsrechtlichen Vorgaben aus Art. 5 Abs. 5 S. 2 KI-VO. Die Berichtspflichten verfolgen zwei zentrale Zwecke: Zum einen sollen sie die zuständigen Aufsichtsbehörden in die Lage versetzen, ihre Kontrollbefugnisse wirksam auszuüben und ihren eigenen Berichtspflichten gegenüber der Europäischen Kommission gemäß Art. 5 Abs. 6 KI-VO nachzukommen, vgl. ErwG 36 KI-VO. Zum anderen dienen sie dem Grundrechtsschutz der von der biometrischen Echtzeit-Fernidentifizierung Betroffener, da durch die Ermöglichung einer effektiven Aufsicht ein transparenter Einsatz des KI-Systems und die Vornahme notwendiger Korrekturen sichergestellt wird.

dd)Verstoß gegen Art. 5 Abs. 2 UAbs. 1 S. 1 i.V.m. Abs. 3 UAbs. 1 S. 2 KI-VO

Maßnahmen nach § 14 Abs. 9 - 11 HSOG verstoßen gegen Art. 5 Abs. 2 UAbs. 1 S. 1 i.V.m. Abs. 3 UAbs. 1 S. 2 KI-VO, da die Eilbefugnis der Polizeibehörde nach § 14 Abs. 11 S. 2 HSOG die unionsrechtlichen Anforderungen an die Eingriffsschwelle unterschreitet sowie Vorgaben fehlen, die die Maßnahme auf das absolut notwendige Mindestmaß beschränken.

(1) Unterschreitung unionsrechtlicher Anforderungen an Eilsituation

Die Eilbefugnis in § 14 Abs. 11 S. 2 HSOG unterschreitet die unionsrechtlichen Anforderungen aus Art. 5 Abs. 3 UAbs. 1 S. 2 KI-VO.

Nach Art. 5 Abs. 3 UAbs. 1 S. 2 KI-VO kann in hinreichend begründeten dringenden Fällen mit der Verwendung eines solchen Systems zunächst ohne Genehmigung begonnen werden, sofern eine solche Genehmigung unverzüglich, spätestens jedoch innerhalb von 24 Stunden beantragt wird. Solche dringenden Fälle sind unionsrechtlich als Situationen definiert, in denen es wegen der Notwendigkeit der Verwendung der betreffenden Systeme tatsächlich und objektiv unmöglich ist, vor dem Beginn der Verwendung des KI-Systems eine Genehmigung einzuholen, vgl. ErwG 35 S. 3 KI-VO.

§ 14 Abs. 11 S. 2 HSOG erlaubt dahingegen die Anordnung der Maßnahmen nach § 14 Abs. 9 HSOG durch die Polizeibehörden schon bei Gefahr im Verzug. Nach verfassungsrechtlicher

Rechtsprechung ist eine Gefahr im Verzug bereits anzunehmen, wenn die vorherige Einholung der gerichtlichen Anordnung den Erfolg der Maßnahme gefährden würde,

> vgl. BVerfG, Urteil vom 20. Februar 2001 - 2 BvR 1444/00 -, NJW 2001, 1121 (1123).

Die Gefahr im Verzug muss mit Tatsachen begründet werden, die auf den Einzelfall bezogen sind. Reine Spekulationen, hypothetische Erwägungen oder lediglich auf kriminalistische Alltagserfahrung gestützte, fallunabhängige Vermutungen reichen nicht aus,

> BVerfG, Urteil vom 20. Februar 2001 - 2 BvR 1444/00 -, NJW 2001, 1121 (1123).

Dabei muss regelmäßig versucht werden, eine Anordnung des instanziell und funktionell zuständigen Richters zu erlangen, bevor eine Durchsuchung begonnen wird. Nur in Ausnahmesituationen, wenn schon die zeitliche Verzögerung wegen eines solchen Versuchs den Erfolg der einer Maßnahme gefährden würde, darf die Behörde selbst die Anordnung wegen Gefahr im Verzug treffen, ohne sich zuvor um eine richterliche Entscheidung bemüht zu haben. Die Strafverfolgungsbehörden dürfen die tatsächlichen Voraussetzungen für die Gefahr im Verzug zudem nicht selbst herbeiführen. Sie dürfen nicht so lange mit dem Antrag an das Gericht zuwarten, bis die Gefahr tatsächlich eingetreten ist,

> vgl. BVerfG, Urteil vom 20. Februar 2001 - 2 BvR 1444/00 -, NJW 2001, 1121 (1123).

Der in § 14 Abs. 11 S. 2 HSOG statuierte Maßstab der „Gefahr im Verzug“ ist damit weitreichender als die unionsrechtlich geforderte „tatsächliche und objektive Unmöglichkeit“. Während das Unionsrecht eine Situation verlangt, in der die vorherige Einholung einer gerichtlichen Anordnung nicht nur erschwert, verzögert oder mit einem Risiko für den Erfolg der Maßnahme verbunden, sondern schlechterdings ausgeschlossen ist, genügt nach § 14 Abs. 11 S. 2 HSOG bereits die Prognose, dass eine vorherige Befassung des Gerichts den Erfolg der Maßnahme gefährden könnte. Unter Eilfällen nach Art. 5 Abs. 3 UAbs. 1 S. 2 KI-VO fallen etwa Situationen sofort bekanntgewordener Kindesentführungen, bei denen ein Zu-

warten auf die Genehmigung die Echtzeit-Fernidentifizierung obsolet machen würde, weil der Täter den Schengen-Raum bereits verlassen haben könnte,

> vgl. *Benedikt*, in: Bomhard/Pieper/Wende, KI-VO, 1. Auflage 2025, Art. 5 Rn. 51.

Eine unionsrechtskonforme Auslegung der Voraussetzung der „Gefahr im Verzug" im Sinne der „tatsächlichen und objektiven Unmöglichkeit" scheidet aus. Eine Auslegung, die ihn auf Fälle objektiver Unmöglichkeit der Einholung einer gerichtlichen Anordnung verengen würde, würde den durch die verfassungsgerichtliche Rechtsprechung ausgeformten Bedeutungsgehalt überschreiten.

Sollte das Gericht die Frage der Unionsrechtswidrigkeit für entscheidungserheblich halten und Zweifel an der richtigen Auslegung des unionsrechtlichen Begriffs der „tatsächlichen und objektiven Unmöglichkeit" bestehen, wird angeregt, dem Gerichtshof der Europäischen Union gemäß Art. 267 AEUV die folgende Vorlagefrage zu unterbreiten:

> Ist Art. 5 Abs. 3 UAbs. 1 S. 2 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 dahin auszulegen, dass er einer nationalen Rechtsvorschrift entgegensteht, die den Einsatz eines biometrischen Echtzeit-Fernidentifizierungssystems ohne vorherige gerichtliche Genehmigung bereits bei „Gefahr im Verzug“ gestattet, d.h. wenn die vorherige Einholung einer gerichtlichen Anordnung den Erfolg der Maßnahme gefährden würde, ohne dass es tatsächlich und objektiv unmöglich ist, vor Beginn der Verwendung des KI-Systems eine Genehmigung einzuholen?

(2) Fehlende Beschränkung auf das absolut notwendige Mindestmaß

Die biometrische Echtzeit-Fernidentifizierung ist unionsrechtswidrig, soweit sie auf eine Eilbefugnis nach § 14 Abs. 11 S. 2 HSOG gestützt wird, da gesetzliche Verfahrensvorschriften fehlen, die die Maßnahme in solchen Fällen angemessen eingrenzen und auf das absolut notwendige Mindestmaß beschränken.

Nach Art. 5 Abs. 3 UAbs. 1 S. 2 KI-VO kann in hinreichend begründeten dringenden Fällen mit der Verwendung eines solchen Systems zunächst ohne Genehmigung begonnen werden, sofern eine solche Genehmigung unverzüglich, spätestens jedoch innerhalb von 24 Stunden beantragt wird. Solche Eilfälle unterliegen jedoch erhöhten Anforderungen, die durch angemessene Schutzvorkehrungen und Bedingungen im nationalen Recht abgesichert sein müssen. Dies wird durch Erwägungsgrund 35 KI-VO verdeutlicht: In solchen dringenden Fällen sollte die Verwendung des KI-Systems auf das absolut notwendige Mindestmaß beschränkt werden und angemessenen Schutzvorkehrungen und Bedingungen unterliegen, die im nationalen Recht festgelegt sind und im Zusammenhang mit jedem einzelnen dringenden Anwendungsfall von der Strafverfolgungsbehörde selbst präzisiert werden,

> vgl. auch Wendehorst, in: Martini/Wendehorst, KI-VO, 1. Auflage 2024, Art. 5 Rn. 179.

In § 14 Abs. 11 S. 2 HSOG fehlen jedoch eigene gesetzlichen Schutzvorkehrungen und Vorgaben für den konkreten Einsatz des biometrischen-Fernidentifizierungssystems in Eilfällen, die über die allgemeinen Anforderungen für den Regelfall nach § 14 Abs. 9 i.V.m. Abs. 11 S. 1 HSOG hinausgehen, wonach die Maßnahme zeitlich und örtlich auf das „unbedingt erforderliche Maß“ zu begrenzen ist. Damit werden die unionsrechtlichen Anforderungen unterschritten, da durch keine detaillierte gesetzliche Regelung sichergestellt wird, dass in diesen Ausnahmefällen die Maßnahme sachlich auf das „absolut notwendige Mindestmaß“ beschränkt ist.

IV. Anregung: Konkrete Normenkontrolle

Da sich die streitentscheidene Norm als verfassungswidrig erweist, wird angeregt, das Verfahren auszusetzen und gem. Art. 100 Abs. 1 GG dem Bundesverfassungsgericht vorzulegen.

Dr. Jasper Prigge, LL.M.
Rechtsanwalt