

# Facial Recognition Through the Lens of National Legislations - Germany\*

Thomas Wischmeyer

(Professor at Bielefeld University, member of the Board of the Institute of the Law of Intelligent Technology Systems (RiT) and of the Advisory Board of the German Chapter of the International Society of Public Law)

Karl Mauer

(PhD., judge (on probation) at Landgericht Potsdam)

---

**ABSTRACT** This article examines the evolving legal landscape surrounding the use of automated facial recognition technologies in Germany. Prompted by recent high-profile events and legislative proposals, the analysis focuses on the regulatory framework, with particular attention to the legal and constitutional boundaries that govern biometric surveillance in public spaces. Drawing on landmark decisions by the Federal Constitutional Court, the article identifies key principles – including proportionality, legal certainty, and informational self-determination – that shape the permissible use of such technologies. It also explores how these principles intersect with recent policy initiatives and the European Union’s AI Act, especially regarding the controversial deployment of real-time biometric identification systems. In light of pending legislative reforms and shifting political dynamics, the article offers a timely overview of Germany’s cautious but consequential approach to balancing technological innovation with fundamental rights in the domain of public security.

---

**KEYWORDS:** Facial Recognition - AI Act - German Constitutional Law - German Police Law - Technology Law

---

**TABLE OF CONTENTS:** 1. Introduction. – 2. The deployment of facial recognition technologies in Germany. – 3. Legal framework for facial recognition in public spaces. – 3.1. Constitutional Law. – 3.2. Developments in Statutory Law and Involvement of Data Protection Authorities. – 4. Perspectives for the Implementation of the AI Act.

---

## 1. Introduction

The use of facial recognition technologies for public security purposes has become a focal point of legal and political debate in Germany. Advocates emphasise the potential of such tools to enhance crime prevention and streamline law enforcement efforts, while critics warn against disproportionate infringements on fundamental rights and the risk of mass surveillance. This article explores how the deployment of facial recognition systems is currently regulated under German law and assesses recent efforts to expand their use. The analysis situates these developments within broader constitutional principles and legal standards - most notably the rights to informational self-determination and proportionality - as articulated by the Federal Constitutional Court. In addition, the article considers the implications of the new EU AI Act, with particular focus on the regulation of biometric real-time remote identification. By tracing the interplay between technological capabilities, legal frameworks, and political considerations, the article aims to clarify where Germany currently stands in the regulation of facial recognition technologies.

## 2. The deployment of facial recognition technologies in Germany

The debate surrounding the use of automated facial recognition in Germany recently gained renewed attention due to the case of Daniela Klette. Accused of involvement in several crimes carried out by the Red Army Faction (RAF) between 1970 and 1998, Klette managed to evade arrest for more than three decades. In early 2024, however, she was finally apprehended in Berlin, where she had been living under a false identity. A reliable police source provided the decisive tip leading to her capture. Following her arrest, it emerged that as early as 2023 two journalists had utilised the facial recognition tool “PimEyes” to search the internet for images of Klette. Their investigation uncovered compelling leads indicating that she was residing in Berlin. Yet, these clues were not pursued by the authorities.<sup>1</sup>

This sparked an intense debate about the powers of state investigative authorities -

---

<sup>1</sup> C. Thönnies, *Daniela Klette und die Frucht der vergifteten Maschine*, in *VerfBlog*, 22 March 2024, <https://verfassungsblog.de/klette-und-die-frucht-der-vergifteten-maschine>.

---

\* Article submitted to double-blind peer review.

Thomas Wischmeyer - Karl Mauer

powers that would not have allowed the use of facial recognition software under the then-current legal framework. The controversy ultimately led the German Bundestag to pass a new law in October 2024. Among other provisions, this legislation empowers the Federal Criminal Police Office (*Bundeskriminalamt*) and the Federal Police (*Bundespolizei*) to conduct biometric comparisons using publicly accessible data, both in the fight against terrorism and for the protection of national borders.<sup>2</sup> Specifically, according to § 10a of the draft law, the Federal Criminal Police Office shall be permitted to perform biometric comparisons of facial and voice data - accessible through automated data processing applications from publicly available personal data on the internet - to supplement existing information, provided this is (1) necessary for the identification or determination of the whereabouts of certain target persons, or (2) if specific facts justify the suspicion that a specifically defined serious offense has been committed or is imminent, or (3) if the prosecution or prevention of the offense would otherwise be hopeless or significantly hindered. Similarly, § 34b of the draft Federal Police Act (BPolG) would allow the Federal Police to perform biometric comparisons of facial and voice data that they are legitimately authorised to process with publicly accessible personal data from the internet using automated data processing applications, provided that (1) it is necessary for the identification or determination of the whereabouts of the target person in the context of countering an existing individual threat to the existence or security of the Federation or a state, or to the life, liberty, or freedom of a person, or to property of significant value whose preservation is in the public interest, and (2) the threat cannot be countered in any other way or would be significantly hindered. However, this legislative initiative was temporarily halted by the second legislative body, the *Bundesrat*.<sup>3</sup> Due to the collapse of the current governing coalition and the subsequent new elections scheduled for February 2025, the political

future of the proposal remains currently uncertain. As a result, German federal security authorities currently do not have any special legislative authorisations for conducting biometric comparisons.<sup>4</sup>

Even prior to these recent legislative efforts, automated facial recognition in Germany had already undergone various practical trials. To date, its utility for law enforcement has mainly been demonstrated through the processing of moving images in the form of ‘intelligent’ biometric video surveillance. As early as 2006, the Federal Criminal Police Office (*Bundeskriminalamt*) launched the “Foto-Fahndung” (Photo Manhunt) project at the main train station in Mainz. This project aimed to explore automated facial recognition as a tool for police investigations.<sup>5</sup> The results indicated that the success of automatically recognising known individuals primarily depends on external factors, particularly adequate lighting of the monitored area.

Building on these insights, the Federal Police conducted a twelve-month project at Berlin’s Südkreuz station between 2017 and 2018. This project tested intelligent video analytics technology intended to automatically detect and identify known individuals within crowds.<sup>6</sup> In a follow-up project launched in 2022, in cooperation with Deutsche Bahn, the analysis was extended to cover additional suspicious scenarios, such as unattended items or individuals lying on the ground.<sup>7</sup> Since 2018, a similar intelligent video system has been tested in Baden-Württemberg and was recently extended for another three years until 2026.<sup>8</sup> This system is designed to recognise

<sup>4</sup> In the context of judicial proceedings, § 81b of the German Code of Criminal Procedure (StPO) permits the collection of biometric data “for the purpose of conducting criminal proceedings” with the aim of enabling the identification of the accused. For the scope of this provision, see most recently the decision of the Federal Court of Justice (BGH) dated March 13, 2025 (Case No. 2 StR 232/24).

<sup>5</sup> Bundeskriminalamt, *Abschlussbericht Fotofahndung*, 2007, 6-7, available at: [www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/FotoFahndung/foto-fahndung\\_node.html](http://www.bka.de/DE/UnsereAufgaben/Forschung/ForschungsprojekteUndErgebnisse/FotoFahndung/foto-fahndung_node.html).

<sup>6</sup> Bundespolizei, *Abschlussbericht Gesichtserkennung*, 2018, 12, available at: [www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011\\_abschlussbericht\\_gesichtserkennung.html](http://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung.html).

<sup>7</sup> Bundesministerium für Digitales und Verkehr, *Pressemitteilung*, 22 July 2022, available at: <https://bmdv.bund.de/SharedDocs/DE/Artikel/K/mehr-sicherheit-im-bahnhof.html>.

<sup>8</sup> W. Kessel, *Pilotprojekt Videoüberwachung mit KI in*

<sup>2</sup> Gesetz zur Verbesserung der Terrorismusbekämpfung, BR-Drs. 512/24, available at [www.bundesrat.de/SharedDocs/drucksachen/2024/0501-0600/512-24.pdf?\\_\\_blob=publicationFile&v=1](http://www.bundesrat.de/SharedDocs/drucksachen/2024/0501-0600/512-24.pdf?__blob=publicationFile&v=1).

<sup>3</sup> See Bundesrat, *Pressemitteilung*, 18 October 2024, available at: [www.bundesrat.de/DE/plenum/bundesrat-kompakt/24/1048/42.html?view=renderNewsletterHtml](http://www.bundesrat.de/DE/plenum/bundesrat-kompakt/24/1048/42.html?view=renderNewsletterHtml).

movement patterns characteristic of violent or property-related offenses committed in public spaces and to automatically track potential suspects. A similar project is also underway in Hamburg.<sup>9</sup> Overall, however, such systems remain significantly less widespread in Germany than abroad - likely due, at least in part, to a heightened sensitivity towards video surveillance in general.<sup>10</sup>

### 3. Legal framework for facial recognition in public spaces

#### 3.1. Constitutional Law

The use of automated facial recognition is limited under the German Basic Law by fundamental rights. Specifically, the primacy of law (*Vorrang des Gesetzes*) the requirement of a statutory provision (principle of legal reservation – *Vorbehalt des Gesetzes*), the principle of legal certainty (*Bestimmtheitsgebot*), and the principle of proportionality (*Verhältnismäßigkeitsgrundsatz*) impose requirements on the formulation of legal norms that restrict the fundamental rights of the individuals concerned for the deployment of such systems through law enforcement agencies, as well as on the justification of each instance of system use.

The principle of legal reservation, derived from the principle of the rule of law, and the principle of legal certainty generally constrain actions by security authorities in such a way that, to the extent they infringe upon citizens' fundamental rights, they must be based on a sufficiently specific legal foundation.<sup>11</sup> All essential decisions in areas sensitive to

fundamental rights are reserved for Parliament as the democratically legitimised legislative body (so-called “essential matters doctrine” - *Wesentlichkeitstheorie*).<sup>12</sup> Moreover, the more intensive the infringement of fundamental rights, the higher the requirements for the specificity of the law. The rule is: the more severe the infringement of fundamental rights and the greater the importance of the affected constitutional rights, the higher the demands on the design and level of detail of the respective parliamentary law.<sup>13</sup>

While there is currently no explicit decision by the Federal Constitutional Court regarding automated facial recognition, indications of the constitutional standards can be derived from the Court's existing jurisprudence. The Court had to address comparable systems in two recent decisions concerning automated license plate recognition (“Second automated license plate recognition decision”)<sup>14</sup> and automated data analysis (“Automated data analysis decision”).<sup>15</sup>

In its landmark decision on automated data analyses through law enforcement authorities from 2023, the Federal Constitutional Court imposed stringent requirements on the specificity of the legal authorisation. In the case, the Court had to decide on statutes from Hamburg and Hesse - two German Länder (states) - that granted security authorities the ability to perform automated analysis of large datasets. The success of such systems largely depends on extremely efficient handling of large amounts of data. To the extent that these data are personal data - which is indisputably the case with automated facial recognition - the rules of data protection must be observed during collection and processing. Therefore, the practice of automated data matching must particularly be measured against the fundamental right to informational self-determination (*Recht auf informationelle*

Mannheim: *Verlängerung bis 2026*, in [www.swr.de](http://www.swr.de), 4 December 2023; Fraunhofer IOSB, *Intelligente Videoauswertung für mehr Sicherheit und Datenschutz*, available at: [www.iosb.fraunhofer.de/de/projekte-produkte/intelligente-videoeueberwachung.html](http://www.iosb.fraunhofer.de/de/projekte-produkte/intelligente-videoeueberwachung.html).

<sup>9</sup> Senat der Stadt Hamburg, Antwort auf eine Kleine Anfrage, 22 March 2024, Drs. 22/14738, available at: [www.buergerschaft-hh.de/parldok/dokument/86838/ergebnisse\\_des\\_pilotprojektes\\_am\\_hansaplatz\\_zur\\_nutzung\\_der\\_intelligenten\\_videoeueberwachung\\_ivbeo.pdf](http://www.buergerschaft-hh.de/parldok/dokument/86838/ergebnisse_des_pilotprojektes_am_hansaplatz_zur_nutzung_der_intelligenten_videoeueberwachung_ivbeo.pdf).

<sup>10</sup> For France see Conseil Constitutionnel, *décision n° 2023-850*, 17 May 2023; see S. Duroy, *Big Brother is Watching the Olympic Games – and Everything Else in Public Spaces*, in [www.verfassungsblog.de](http://www.verfassungsblog.de), 22 March 2023; for a description of the “Domain Awareness System” in Manhattan see T. Rademacher, *Artificial Intelligence and Law Enforcement*, in T. Wischmeyer and T. Rademacher (eds.), *Regulating Artificial Intelligence*, Cham, Springer, 2020, 228.

<sup>11</sup> See BVerfG, *Judgment of the Second Senate of 6 July 1999 – 2 BvF 3/90*, para. 124, [www.bverfg.de/e/19990706\\_2bv000390](http://www.bverfg.de/e/19990706_2bv000390).

<sup>12</sup> BVerfG, *Judgment of the Second Senate of 8 August 1978 – 2 BvL 8/77*, see BVerfGE 49, 89, especially 126.

<sup>13</sup> BVerfG, *Judgment of the Second Senate of 8 August 1978 – 2 BvL 8/77*, see BVerfGE 49, 89, especially 126.

<sup>14</sup> BVerfG, *Order of the First Senate of 18 December 2018 – 1 BvR 142/15*, [https://www.bverfg.de/e/rs20181218\\_1bvr014215en](https://www.bverfg.de/e/rs20181218_1bvr014215en).

<sup>15</sup> BVerfG, *Judgment of the First Senate of 16 February 2023 – 1 BvR 1547/19*, [https://www.bverfg.de/e/rs20230216\\_1bvr154719en](https://www.bverfg.de/e/rs20230216_1bvr154719en).

*Selbstbestimmung*), which constitutes the central fundamental right for the design of AI-based systems. In view of the significant infringement on the fundamental right to informational self-determination that such data analyses involve (more on this shortly), especially within security administration, the Court requires a danger to particularly significant legal interests such as life, health, or personal freedom; moreover, this danger must be sufficiently specified.

From the relevant case law, it follows first and foremost that any state-operated video surveillance generally requires a statutory basis. However, no blanket statement can be made about the specific form this legal foundation must take. In certain constellations, the intensity of the interference is considered minimal, for instance, when surveillance measures do not produce any tangible effects on the individuals concerned. Under such circumstances, general clauses contained in police or data protection law may be regarded as sufficiently specific to meet the requirements for a legal basis. An example would be public video surveillance aimed solely at identifying certain objects or abstract behavioral patterns, without focusing on individual persons.<sup>16</sup> At the same time, it is evident that the use of AI systems under more intrusive circumstances calls for a special statutory authorisation.<sup>17</sup> This applies particularly when such systems (as in the pilot projects described above) are designed to link newly generated data with existing datasets to identify specific individuals. In these instances, general clauses will typically not meet the constitutionally required standards.

Even when a sufficiently specific legal

<sup>16</sup> One example to consider is a practical case from Munich involving video surveillance in public swimming pools, where AI-based cameras are used to support lifeguard personnel by helping to recognise a person in distress, [www.sueddeutsche.de/muenchen/muenchen-sendling-suedbad-kuenstliche-intelligenz-rettungsschwimmer-1.5640556](http://www.sueddeutsche.de/muenchen/muenchen-sendling-suedbad-kuenstliche-intelligenz-rettungsschwimmer-1.5640556). For another case see <https://www.swr.de/swraktuell/baden-wuerttemberg/mannheim/videoueberwachung-kameras-videoschutz-polizei-mannheim-innenstadt-sicherheit-strobl-100.html>.

<sup>17</sup> As well: A. Kulick, „Höchstpersönliches Merkmal“ – *Verfassungsrechtliche Maßstäbe der Gesichtserkennung*, in *Neue Zeitschrift für Verwaltungsrecht*, Issue 22, 2020, 1622, especially 1624; J. Mysegades, *Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage*, in *Neue Zeitschrift für Verwaltungsrecht*, Issue 12, 2020, 852, especially 853. Different: VG Hamburg, Judgment of 23.10.2019 – 17 K 203/19, BeckRS 2019, 40195, paras 83-109, especially paras. 89-90.

basis is in place, the use of automated facial recognition must still be proportionate. Due to the increasing and continuously expanding storage capacities of the employed AI systems, it could soon be possible to record the faces of a large number of individuals and create personalised movement profiles. This falls within the scope of the right to informational self-determination under Article 2(1) in conjunction with Article 1(1) of the Basic Law. This right extends beyond an individual's private sphere to also protect their behavior in public spaces.<sup>18</sup> Ultimately, the justification depends on whether the statutory authorisation to interfere is proportionate when weighed against the protected legal interests, with the intensity of the interference serving as the decisive criterion.

In its “Second decision on automated license plate recognition,” the Federal Constitutional Court further refined its standards concerning both the intensity of interference and the justification required for system-based surveillance measures. This decision examined provisions of the Bavarian Police Tasks Act that authorised the use of automatic license plate recognition systems, primarily on highways. Each year, relying on this legal basis, millions of license plates were scanned, translated into digital data, and compared against databases of wanted individuals. When no match was found, the information was immediately deleted. Nonetheless, these systems proved to be error-prone, with false-positive rates reaching up to ninety percent.<sup>19</sup> Departing from its earlier jurisprudence, the Court held that even non-matches - despite the immediate deletion of data - constitute an interference with the fundamental rights of vehicle owners, thereby requiring justification.<sup>20</sup> The Court reasoned

<sup>18</sup> Established jurisprudence since BVerfG, *Order of the First Senate of 15 December 1983 - 1 BvR 209/83*, para. 45 and *passim*, [www.bverfg.de/e/rs19831215\\_1bvr020983en](http://www.bverfg.de/e/rs19831215_1bvr020983en). Under no circumstances is the consent of the data subject to be seen in the fact that they are in a place where systems for automated video recognition are recognisably installed (A. Kulick, „Höchstpersönliches Merkmal“ – *Verfassungsrechtliche Maßstäbe der Gesichtserkennung*, 1624).

<sup>19</sup> C. Rath, *Scanner greifen in Grundrechte ein*, in [www.lto.de](http://www.lto.de), 5 February 2019.

<sup>20</sup> BVerfG, *Order of the First Senate of 18 December 2018 - 1 BvR 142/15 -*, paras. 43-53; to that: A. Kulick, „Höchstpersönliches Merkmal“ – *Verfassungsrechtliche Maßstäbe der Gesichtserkennung*, 1624; S. Schindler, *Biometrische Videoüberwachung*, 2021, Baden-Baden, Nomos, 324.

that personal freedom includes the right to move freely “without having to account for one’s law-abiding behaviour.”<sup>21</sup> Applied to automated facial recognition, this conclusion means that the fundamental rights of passersby are also affected, even if their data does not produce a match and is immediately erased.

Such infringements of fundamental rights require justification under German constitutional doctrine. In its second decision on automated license plate recognition, the Federal Constitutional Court provided also more nuanced guidance on the criteria by which the questions regarding the intensity of interference from system use can be answered. These criteria include (1) the purpose of data collection, (2) the circumstances under which it is carried out, (3) the scope of the measure, (4) the type and significance of the data sets used in comparisons, and (5) the nature of the information collected.<sup>22</sup>

While it is not possible here to examine each criterion in detail, the following insights on automated facial recognition can be drawn from the decisions:

Firstly, with respect to the type of information collected, the Court’s reasoning suggests it was already considering more sensitive (AI) technologies, including automated facial recognition. In fact, the Federal Constitutional Court explicitly notes that a particularly high level of interference arises when “highly personal characteristics, such as the face,” are involved.<sup>23</sup> Thus, the more personal the data being collected, the greater the intensity of the interference, and consequently, the more demanding the justification required for using the system. The court does not explicitly address whether the real-time deployment of facial recognition technologies in public spaces would be excluded, but it appears very likely that a boundary would be drawn in this regard.

Secondly, in light of these considerations, deploying such a system without a specific cause is generally ruled out. The judges deem its use justified only if it is tied to the “control of special sources of danger” (*Beherrschung*

*besonderer Gefahrenquellen*).<sup>24</sup> Accordingly, serious doubts arise about the permissibility of automated facial recognition absent a particular reason for its deployment. In the Court’s view, the grounds for using such a system are a decisive factor when determining its permissibility under proportionality standards. Since automated facial recognition constitutes a particularly intensive encroachment on fundamental rights due to its focus on highly personal characteristics, justifying its application without a special cause appears difficult.<sup>25</sup> This concern is especially pertinent if automated facial recognition is employed not to address a specific danger or prevent a particularly serious offense, but merely as an investigative tool for tracking down wanted individuals.

Even aside from these considerations, justifying the use of automated facial recognition proves challenging if the system is deployed covertly. If those affected cannot perceive its operation and a wide range of individuals are monitored, this implies a high intensity of interference and, consequently, stringent justification requirements. According to the Federal Constitutional Court, in this case, the deployment of the system means that facial recognition “could affect anyone and everyone,” thereby creating a general “feeling of being watched.”<sup>26</sup> This is an argument known from the context of mass surveillance jurisprudence.

The Court also addresses the territorial scope of deployment in this context. Generally, the system’s use must be spatially limited, although this requirement becomes less critical “the more serious and urgent the danger to be averted in the individual case” is.<sup>27</sup> However, according to the Court, a “blanket” deployment that would cover an “unlimited area” is categorically prohibited.<sup>28</sup> It remains unclear, though, at what point such a deployment would be considered blanket.<sup>29</sup>

<sup>21</sup> BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15 -, para. 51.

<sup>22</sup> BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15 -, para. 53.

<sup>23</sup> BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15 -, para. 53.

<sup>24</sup> BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15 -, para. 94.

<sup>25</sup> A. Kulick, „Höchstpersönliches Merkmal“ – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, 1626.

<sup>26</sup> BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15, para. 98.

<sup>27</sup> BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15, para. 100.

<sup>28</sup> BVerfG, Order of the First Senate of 18 December 2018 - 1 BvR 142/15, para. 100.

<sup>29</sup> A. Kulick, „Höchstpersönliches Merkmal“ – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, 1627.

### 3.2. Developments in Statutory Law and Involvement of Data Protection Authorities

Although previous experiences with the effectiveness of automated facial recognition systems have been mixed, the technology remains highly appealing to domestic policymakers.

The most recent federal legislative initiative to grant security agencies the ability to perform biometric comparisons of publicly accessible data has already been noted above. To this end, appropriate authorisation provisions are to be integrated in the Federal Criminal Police Office Act (BKAG), the Federal Police Act (BPolG), and the Code of Criminal Procedure (StPO): §§ 10b, 39a, 63b of the draft BKAG, § 34b of the draft BPolG, § 98d of the draft StPO.<sup>30</sup>

At the state level, automated facial recognition is sometimes employed without a specific legal basis.<sup>31</sup> However, under continuous scrutiny from both federal and state data protection commissioners, various state legislatures have introduced new laws.<sup>32</sup> These laws allow the police, on a case-by-case basis, to further process lawfully collected personal data using automated applications for the preventive combat of serious crimes or the defense against qualified dangers, and to analyse previously unconnected data sets on data platforms to establish connections between individuals, groups, or institutions. In Bavaria and Baden-Württemberg, Article 33(5) of the BayPAG (Bayerisches Polizeiaufgabengesetz) and § 44(4) of the PolG BW (Polizeigesetz Baden-Württemberg) permit the automated evaluation and matching of biometric data.<sup>33</sup> In Saxony, § 59 of the

SächsPVDG (Sächsisches Polizeivollzugsdienstgesetz), introduced for the same purpose, expired at the end of 2023. As a result, the practice of automated facial recognition there now relies – despite the aforementioned uncertainties regarding general clauses – on the rather vague § 57 SächsPVDG as well as on § 98c of the Federal Criminal Procedure Act (*Strafprozessordnung*).<sup>34</sup>

In detail, the state-level regulations differ in their focus: Some provisions authorise the filming of certain objects only (Art. 33 sec. 5 BayPAG), while others also encompass the behavior of passersby (§ 44 sec. 4 PolG BW). What these norms share is their technology-neutral design, even though the legislature typically had a particular technology in mind when establishing the provision.<sup>35</sup>

### 4. Perspectives for the Implementation of the AI Act

During the drafting of the AI Act, the use of automated facial recognition was a subject of intense debate. Initially, a strict ban was considered, but in its final form, the Act confines itself to imposing restrictive requirements on a specific subset of such technologies – so-called biometric real-time remote identification systems (Article 3(42) AI Regulation) – as addressed by Article 5(h) of the AI Regulation. Only for these systems does the Regulation establish a prohibition, and even then, it includes not insignificant exceptions.

In Germany, this regulatory framework, coupled with the remaining leeway granted to national legislators, is now the focus of extensive debate. While some argue against a strict ban, citing concerns about technological

<sup>30</sup> Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, 9 September 2024, BT-Drs. 20/12806, available at: <https://dserver.bundestag.de/btd/20/128/2012806.pdf>.

<sup>31</sup> See for the example of the German State of Brandenburg: [www.rbb24.de/content/rbb/r24/politik/beitrag/2024/08/brandenburg-polizei-gesichtserkennung-ermittlungen-software-kritik.html](http://www.rbb24.de/content/rbb/r24/politik/beitrag/2024/08/brandenburg-polizei-gesichtserkennung-ermittlungen-software-kritik.html).

<sup>32</sup> See Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Entschließung, 20 September 2024, available at: [www.ldi.nrw.de/datenschutzkonferenz-vorsicht-bei-dem-einsatz-von-gesichtserkennungssystemen-durch](http://www.ldi.nrw.de/datenschutzkonferenz-vorsicht-bei-dem-einsatz-von-gesichtserkennungssystemen-durch).

<sup>33</sup> See A. Kulick, „Höchstpersönliches Merkmal“ – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, 1622; S. Schindler, *Biometrische Videoüberwachung*, Baden-Baden, Nomos, 2021; S.J. Golla, *KI-Einsatz bei der Polizei*, in K. Chibanguza, C. Kuß and H. Steege (eds.), *Künstliche Intelligenz*, Baden-Baden, Nomos, 2022, § 9 paras. 32-37; for a

special situation M. Martini, B. Thiessen and J. Ganter, *Digitale Versammlungsbeobachtung*, Berlin, Duncker & Humboldt, 2023.

<sup>34</sup> After a legally mandated evaluation, the Saxon Ministry of the Interior declared in August 2023 that the technical and personnel effort was in too great a discrepancy with the practical success in operation; an “extension of this provision would thus not be proportionate.” See Sächsisches Staatsministerium des Innern, Pressemitteilung, 22 August 2023, available at: [www.medien-service.sachsen.de/medien/news/1068787](http://www.medien-service.sachsen.de/medien/news/1068787); the Saxon Data Protection and Transparency Commissioner criticises the practice overall, Pressemitteilung, 24 September 2024, available at: [www.datenschutz.sachsen.de/gesichtserkennung-in-sachsen-ist-ein-tiefer-eingriff-in-die-grundrechte-7293.html](http://www.datenschutz.sachsen.de/gesichtserkennung-in-sachsen-ist-ein-tiefer-eingriff-in-die-grundrechte-7293.html).

<sup>35</sup> S.J. Golla, *KI-Einsatz bei der Polizei*, § 9 paras. 33, 35.

progress and the effectiveness of security authorities, others call for more restrictive national regulations. The spectrum of demands ranges from prohibiting use by private actors<sup>36</sup> to completely outlawing the technology.<sup>37</sup>

Experts also dispute more fundamental questions, such as whether - and how - to differentiate between biometric real-time remote identification systems and those designed for subsequent remote identification. With elections scheduled for February 2025, it remains unclear how German lawmakers will utilise their national margin of discretion. One thing is certain, however: as of 2 February 2025, the intricate provisions of Article 5(h) of the AI Regulation will apply in Germany as well.

---

<sup>36</sup> L. Ehrig, *Stellungnahme*, 8 May 2024, 3-4, available at: [www.bundestag.de/dokumente/textarchiv/2024/kw20-pa-digitales-ki-1001728](http://www.bundestag.de/dokumente/textarchiv/2024/kw20-pa-digitales-ki-1001728).

<sup>37</sup> K. Vieth-Ditlman, *Stellungnahme*, 13 May 2024, 5-9, available at: [www.bundestag.de/dokumente/textarchiv/2024/kw20-pa-digitales-ki-1001728](http://www.bundestag.de/dokumente/textarchiv/2024/kw20-pa-digitales-ki-1001728).

