13

Facial Recognition Technologies in the Public Sector

Observations from Germany

Andreas Engel

13.1 INTRODUCTION

Facial recognition technologies (FRTs) have raised concerns in Germany,[1] and have not been put to use on a widespread basis. This may not be expected to change in the near future, as the current coalition treaty between the German government parties rejects comprehensive video surveillance and the use of biometric measurement for surveillance purposes.[2]

This reluctance to put FRT to use may explain why, so far, the use of FRT has seldom come before German courts: Only fifty-three court decisions out of a total of 1.6 million decisions of German courts in the legal database *juris* include a textual reference to 'Gesichtserkennung', the German term for facial recognition.[3] A search for 'Biometrie', equivalent to 'biometrics', yields 991 decisions.[4] However, many of these latter decisions only have a tenuous link to FRT. These numbers suggest that FRT has rarely been the subject-matter of legal proceedings in Germany.

Nevertheless, there are individual instances in which FRT is already being employed – or has been employed – in the public sphere in Germany. Three prime

[1] See, e.g., Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 'Bundesdatenschutzbeauftragter mahnt Zurückhaltung bei Gesichtserkennung an' (2019), www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2019/02_Zur%C3%BCckhaltungbeiGesichtserkennung.html; Dirk Heckmann, 'Gesichtserkennung muss streng reguliert werden' (2020), jurisPR-ITR 16/2020 Anm. 1; see also Marie-Theres Tinnefeld, '… fertig ist das Gesicht – eine Betrachtung im Spiegel digitaler Gesichtserkennungssysteme' (2018) *MMR* 777; Amélie P. Heldt, 'Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raum' (2019) *MMR* 285. Note that the manuscript was, by and large, finalized in December 2022, with only minor edits being made in the subsequent publishing process.

[2] Koalitionsvertrag 2021–2025 zwischen SPD, Bündnis 90/Die Grünen und FDP, pp. 15, 86, www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800.

[3] The search via www.juris.de was conducted on 15 September 2022. For the relevance and limitations of such searches, see, e.g., Andreas Engel, 'The ECHR in the German Legal System – A qualitative and quantitative introduction' in Matteo Fornasier and Marella Stanzione (eds.), *The European Convention on Human Rights and Its Impact on National Private Law: Italo-German Perspectives* (Intersentia, 2023), parts 3.1 and 3.2.

[4] The search via www.juris.de was conducted on 15 September 2022.

https://doi.org/10.1017/9781009321211.016 Published online by Cambridge University Press

examples of real-life use cases of FRT in the public sector in Germany will be discussed in further detail.

The first example concerns the pilot study involving the continuous use of FRT without specific cause, conducted at the Berlin Südkreuz train station (which has received a high degree of public attention). The second example is the use of FRT in the aftermath of the G20 riots in Hamburg. Here, FRT was employed to analyse video recordings from mass gatherings to identify suspects. As a third example, FRT cameras are being used in the city of Görlitz to combat serious border crime. In Görlitz, FRT is employed for a limited time and for specific cause. Hence, these examples illustrate different scenarios of the application of FRT. They will be discussed in turn to illustrate specific requirements and challenges, particularly with a view to the varying degree of detail of relevant legal provisions.

13.2 CONSTITUTIONAL FRAMEWORK FOR FRT IN THE PUBLIC SECTOR IN GERMANY

All cases of FRT use take place within the constitutional framework of the Grundgesetz (Basic Law – GG). FRT mainly raises concerns with regard to the right to informational self-determination (Art. 2 (1) in conjunction with Art. 1 (1) GG), which has first been recognised in a decision by the Bundesverfassungsgericht (Federal Constitutional Court – BVerfG) on the 1983 Federal Census Act.[5] Additionally, and depending on the specific context, FRT may affect other fundamental rights, such as the right to assemble (Art. 8 (1) GG).[6] And, even more fundamentally, the BVerfG has acknowledged that the constitution entails a ban on total surveillance,[7] and underlines its importance as part of Germany's constitutional identity: 'It is an integral part of the constitutional identity of the Federal Republic of Germany that the state may not record and register the exercise of freedoms by citizens in its entirety.'[8] So far, the BVerfG has not decided a case that directly involved the use of FRT. Absent a pertinent judgment, a recent decision by the BVerfG on automatic licence plate recognition (ALPR) may provide orientation, and guidelines for FRT can be derived *a fortiori* from this decision.[9] As Martini points out, both ALPR and FRT aim

[5] BVerfGE 65, 1; for a recent discussion see, e.g., Philipp Lassahn, 'Datenschutz und Personenschutz' (2022) 61 *Der Staat* 407.

[6] See in particular Heldt, 'Gesichtserkennung', 285, 288. On issues of discrimination, see Stephan Schindler, *Biometrische Videoüberwachung* (Nomos, 2021), pp. 641–666.

[7] See also Timo Rademacher, '*Predictive Policing* im deutschen Polizeirecht' (2017) 142 *AöR* 366, 399 et seq. for an extensive discussion of the reasons for such a ban in the context of predictive policing.

[8] BVerfGE 125, 260, 324, para. 218, translation provided by the BVerfG, www.bverfg.de/e/rs20100302_1bvr025608en.html; see Mario Martini, 'Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit' (2022) 41(1–2) *NVwZ-Extra* 7 fn. 97 with further references to the jurisprudence of the BVerfG.

[9] BVerfGE 150, 244; cf. Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', 7; Stephan Schindler, 'Noch einmal: Pilotprojekt zur intelligenten Videoüberwachung am Bahnhof Berlin Südkreuz' (2017) ZD-Aktuell 5799; for an in-depth-comparison, see Schindler, Biometrische Videoüberwachung, pp. 199–201.

at automated surveillance of the public sphere and would lend themselves as tools for permanent surveillance.[10] Personal data collected via ALPR or FRT can be used to draw inferences about the persons monitored.[11] While ALPR uses information that may indirectly relate to persons, FRT surveillance directly pertains to biometric data. Thus, even higher legal standards would apply to FRT than for ALPR.[12]

Specifically, in its decision on ALPR, the BVerfG has first ascertained the broad scope of the right to informational self-determination (which would be relevant both for ALPR and FRT): 'The right to informational self-determination covers threats and violations of personality that arise for the individual from information-related measures, especially under the conditions of modern data processing.'[13]

The right to informational self-determination applies even in the public sphere, where individuals have an interest in ensuring that their personal information is not collected and stored without their consent (which, again, equally concerns ALPR and FRT): 'Even when individuals go out in public, the right to informational self-determination protects their interest in ensuring that the associated personal information is not collected in the course of automated information collection for storage with the possibility of further exploitation.'[14]

Different stages of data processing have to be distinguished and need respective justification, in particular the collection, the storage and the use of data: 'Regulations that allow for the handling of personal data by government authorities generally justify various interventions that build on each other. In particular, a distinction must be made in this respect between the collection, storage and use of data.'[15]

For all stages of data processing, the basic principles of proportionality, clarity of legal rules, and certainty apply:[16]

> As encroachments on the right to informational self-determination, authorizations for automated license plate checks must be measured against the principle of proportionality. Accordingly, they must pursue a legitimate purpose, be suitable for achieving the purpose, necessary and proportionate in the strict sense of the term. At the same time, they must comply with the principles of clarity of legal rules and certainty, particularly in the area of data processing.[17]

[10] Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', p. 7.
[11] Ibid.
[12] But see VG Hamburg, BeckRS 2019, 40195 para. 104–105, hinting at a possible distinction for cases where FRT is applied in the context of crime.
[13] BVerfGE 150, 244, para. 37.
[14] Ibid., para. 39.
[15] Ibid., para. 42.
[16] Regarding the basic principles of proportionality, see, e.g., Bernd Grzeszick, 'Art. 20 GG' in Rupert Scholz, Matthias Herdegen, and Hans H. Klein (eds.), *Dürig/Herzog/Scholz, Grundgesetzkommentar* (98th ed., CH Beck, 2022), paras 109 et seq. with further references. Regarding clarity of legal rules, see, e.g., Udo di Fabio, 'Art. 2 GG' in Dürig/Herzog/Scholz, Grundgesetzkommentar, para. 184, 186. Regarding certainty, see, e.g., Bernd Grzeszick, 'Art. 20 GG' in Dürig/Herzog/Scholz, Grundgesetzkommentar, paras 58 et seq. with further references, also on the relation between legal clarity and certainty.
[17] BVerfGE 150, 244, para. 82.

https://doi.org/10.1017/9781009321211.016 Published online by Cambridge University Press

Proportionality in this context is understood in a narrower sense, as a prohibition of excessiveness. The pursued purpose must be proportionate to the impact on the individuals' right to informational self-determination (the comparatively deeper impact of FRT on individual rights would affect this analysis accordingly, and a more important purpose would be required): 'The principle of proportionality in the narrower sense as a prohibition of excessiveness is only satisfied … if the purpose pursued is not disproportionate to the weight of the intervention entailed.'[18] To be justified, automated licence plate checks must be prompted by a sufficiently concrete, objectively determined reason. Furthermore, the conditions for a check must meet a certain threshold and allow for compliance review.[19] Checks cannot be carried out arbitrarily or without a valid reason.

Furthermore, the BVerfG stressed that surveillance measures must serve 'to protect legal interests of at least considerable weight or a comparably weighty public interest'.[20] It is crucial to note that FRT raises additional concerns about privacy and the potential for misuse. Thus, the standard for the use of FRT would be higher than for automated licence plate checks.

Moreover, the general framework for surveillance measures must also be proportionate in a broader sense of the term; that is, in an overall assessment:

> In this respect, the legislature must preserve the balance between the type and intensity of the impairments of fundamental rights on the one hand and the causes justifying the interference on the other hand, for instance by establishing requirements regarding the threshold for the exercise of powers, the necessary factual basis, or the weight of the protected legal interests.[21]

From these considerations, the BVerfG derives more specific procedural requirements to protect individual rights: 'In addition, the proportionality requirements include requirements relating to transparency, individual legal protection and supervisory control as well as regulations on data use and deletion for all individual acts.'[22]

13.3 APPLICATION IN SPECIFIC FRT USE CASES

This general framework sets the standard for the application of FRT in specific cases and its legal basis. In this section, the chapter discusses in turn the aforementioned instances in which FRT has already been applied: a pilot study that entailed the continuous use of FRT without specific cause at Berlin Südkreuz (Section 13.3.1), the use of FRT for analysis of video recordings from mass gatherings at the G20

[18] Ibid., para. 90.
[19] Ibid., paras 91, 112.
[20] Ibid., para. 95.
[21] Ibid., para. 100.
[22] Ibid., para. 101.

https://doi.org/10.1017/9781009321211.016 Published online by Cambridge University Press

summit in Hamburg (Section 13.3.2), and the use of FRT for a limited time and with specific cause in the city of Görlitz (Section 13.3.3).

13.3.1 *Permanent Use of FRT without Specific Cause*

The federal police (Bundespolizei) from 2017 to 2018 conducted a study at Berlin Südkreuz train station to test the feasibility of the permanent use of FRT in the public sector.[23] The study comprised two phases and was conducted with volunteer test subjects. A reference database was built with pictures of these subjects. During the study, the participants passed by the cameras at Berlin Südkreuz train station and were thus monitored.

As its main conclusion from the study, the federal police stated that the technology employed makes it possible to detect and identify people in crowds automatically.[24] The federal police considered the test scores of the systems as 'excellent' ('*ausgezeichnet*'):[25] During phases 1 and 2 of the study, the average hit rate of the three individual systems employed was 68.5 per cent and 82.8 per cent, respectively. The average false hit rate was 0.12–0.25 per cent in phase 1 and 0.07 per cent in phase 2. The overall system – interconnecting the three individual systems – had an average hit rate of 84.9 per cent in phase 1 and 91.2 per cent in phase 2, with a false hit rate of 0.67 per cent and 0.34 per cent, respectively. These results indicate that the individual and overall systems had relatively high hit rates, with relatively low rates of false hits.

Against this background, the federal police concluded that 'the state of the art FRT systems … can make a valuable contribution to ensuring security in train stations',[26] indicating a positive attitude towards a potential future use of FRT.

Notably, FRT measures at a train station, such as Berlin Südkreuz, would arguably not conflict with the ban on total surveillance.[27] Even if, at the specific venue, FRT is employed permanently and without specific cause, its application would not cover the exercise of freedoms by citizens in its entirety: As FRT is only used at a specific venue, it only serves to monitor citizens at this venue, but not their conduct elsewhere.[28]

[23] See, generally, Bundespolizeipräsidium Potsdam, 'Biometrische Gesichtserkennung' des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz – Abschlussbericht – p. 36 et seq, www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=37519C29A2E21493673F09F9BD416715.1_cid289?__blob=publicationFile&v=1; Schindler, 'Pilotprojekt zur intelligenten Videoüberwachung'; Kai Wendt, 'Einsatz von intelligenter Videoüberwachung: BMI plant Testlauf an Bahnhöfen' (2017) *ZD-Aktuell* 2017, 5724; Schindler, Biometrische Videoüberwachung, pp. 195 et seq. (and pp. 190 et seq. for further examples).

[24] Bundespolizeipräsidium Potsdam, 'Biometrische Gesichtserkennung', p. 7.

[25] Ibid., pp. 7–8, 23 et seq.; for a more critical view, see the assessment by the Chaos Computer Club, Germany's largest association of hackers, www.ccc.de/en/updates/2018/debakel-am-suedkreuz.

[26] Bundespolizeipräsidium Potsdam, 'Biometrische Gesichtserkennung', p. 38.

[27] Cf. BVerfGE 125, 260 (324, para. 218).

[28] Cf. Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', pp. 7–8.

For the pilot study, the monitored individuals had consented beforehand to the use of FRT. However, without such consent, future permanent employment of FRT without specific cause would need a legal basis consistent with individuals' constitutional rights and legal protections.

At first glance, an existing provision might cover such cases. According to Sec. 27, sentence 1 no. 2 Bundespolizeigesetz (Law on Federal Police – BPolG), which has a broad scope of application, 'the federal police may use automatic image capture and image recording devices to … detect dangers to [certain specified objects, including train stations or airports], or to persons or property located there'.[29]

However, Sec. 27, sentence 1 no. 2 BPolG does not address FRT specifically and does not meet the procedural requirements that the BVerfG outlined for ALPR, such as transparency, individual legal protection, and supervisory control or regulations on data use and deletion for all individual acts. While BPolG does contain procedural rules (see in particular Sec. 29 et seq. BPolG on data processing and data use), arguably more specific provisions would be required for FRT,[30] as the permanent use of FRT at specific venues would amount to a new level of intensity.[31]

Similar problems arise for provisions in police laws of the Länder (German states) that allow video recordings in general but are not written for FRT specifically.[32]

13.3.2 *Use of FRT for Analysis of Video Recordings from Mass Gatherings*

A second example, which has even been before a court, concerns the use of FRT for specific cause, the analysis of videos of riots. Hamburg police collected video and image files of the riots at the July 2017 G20 summit in Hamburg.[33] These videos and photos were partly taken by the police themselves, partly from video surveillance recordings from certain S-Bahn stations, partly from relevant recordings accessible on the internet, and partly from privately created image files.[34] The files collected were merged into one large collection of images. Using facial recognition software (which had been specially procured), the police created a reference database that contained digital (biometric) extracts of the faces ('templates') that had been identified by the software in the images of the basic file.[35] The number of templates in

[29] On this provision and FRT, see ibid., pp. 8–9 (with a discussion of further provisions at pp. 9–11).

[30] Ibid., p. 8.

[31] Ibid., p. 6; Schindler, 'Biometrische Videoüberwachung', pp. 608–613.

[32] See the list of provisions at Michael W. Müller and Thomas Schwabenbauer, 'G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht' in Matthias Bäcker, Erhard Denninger, and Kurt Graulich (eds.), *Handbuch des Polizeirechts* (7th ed., CH Beck, 2021), paras 662 (video surveillance in general) and 672 (video surveillance of objects in danger). See, in more detail, Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', p. 9.

[33] On the riots, see, e.g., www.dw.com/en/raids-in-four-european-countries-over-hamburg-g20-riots/a-43969633.

[34] VG Hamburg, BeckRS 2019, 40195, para. 3; see also Schindler, Biometrische Videoüberwachung, pp. 214–216.

[35] VG Hamburg, BeckRS 2019, 40195, para. 4.

https://doi.org/10.1017/9781009321211.016 Published online by Cambridge University Press

the database supposedly exceeded 100,000.[36] The database was not connected to or linked with other official databases.

For individual search sweeps, the police made the images of individual crime suspects file-compatible with this software and fed them into the reference database. Hits identified and flagged by the software were further confirmed by clerks. The individual search runs took place on the order of the public prosecutor's office.[37]

The Hamburg Commissioner for Data Protection and Freedom of Information ordered the police to delete this database. Whether this order was lawful hinged upon, inter alia, whether the creation and use of this database conformed with data protection laws.

The Verwaltungsgericht Hamburg (Hamburg Administrative Court – VG Hamburg) held that the order was unlawful. The court saw Sec. 48 (1) Bundesdatenschutzgesetz (Federal Data Protection Act – BDSG) as a sufficient legal basis for the measures in question, even though the provision is written in very broad terms: 'The processing of special categories of personal data [which includes biometrical data, Sec. 46 no. 14 BDSG] is only permitted if it is absolutely necessary for the performance of the task.' According to the VG Hamburg, 'Sec. 48 (1) BDSG is unquestionably a provision on data protection.'[38] According to the court, no more specific legal provision existed for the processing of personal data carried out by the police. Therefore, the court held the provision to be applicable.[39]

Consequently, the VG had to assess whether the use of FRT in this context was 'absolutely necessary' in the sense of Sec. 48 (1) BDSG. The court concluded it was, as a similar review of the data collected by humans would require far too much time and hence would not be a feasible alternative:

> [T]he plaintiff argues … that processing the image material contained in the basic file by human evaluators would far exceed the time frame for effective criminal prosecution and would take years. The defendant does not dispute the validity of this consideration … Thus, it is self-evident to consider the establishment and use of the reference database as indispensable.[40]

[36] Jan Mysegades, 'Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage' (2020) *NVwZ* 852.

[37] VG Hamburg, BeckRS 2019, 40195, para. 5.

[38] Ibid., para. 75.

[39] Ibid., para. 75. Holger Greve, '§ 48 BDSG' in Martin Eßer, Philipp Kramer and Kai von Lewinski (eds.), *Auernhammer, DSGVO/BDSG* (8th ed., Carl Heymanns, 2023), para. 5 explains in more detail that the use of general clauses is acceptable even in the law of data protection. Greve argues that in cases where fundamental rights are gravely affected by new technologies, Sec. 48 BDSG can apply only for an interim period until the legislator has had the time to draft a more specific provision: Ibid., para 8. For a broader and deeper analysis of the role of general clauses in data protection law, see Nikolaus Marsch and Timo Rademacher 'Generalklauseln im Datenschutzrecht' (2021) 54 *Die Verwaltung* 1, with similar conclusions.

[40] VG Hamburg, BeckRS 2019, 40195, para. 81.

In a second step, the VG considered the constitutionality of the relevant provision.[41] The court held it was decisive that the Hamburg Commissioner for Data Protection and Freedom of Information had not sufficiently engaged with Sec. 48 (1) BDSG and had not tried to come to an interpretation of the norm that would conform with the constitution.[42] The court pointed to a set of aspects that would have merited further analysis by the commissioner.

Among these, the following aspects are of particular interest in the present enquiry: The VG observed that closer scrutiny of the measure's impact on constitutional rights would have been required and that the measure in question might be distinguishable from surveillance without a specific reason. In that context, the court remarked that in the individual search runs, the software would not use further, but suppress, biometric data of the large number of unsuspected persons.[43] Moreover, the court contrasted the measures taken by the police with ALPR, which would amount to a structure that citizens might view as a system of general surveillance. The court pointed out that the analysis of a given set of videos from a specific event might not trigger the exact same concerns.[44]

This decision raised heavy criticism, in particular by Mysegades.[45] Mysegades argues that even in view of the primacy of the law,[46] if Sec. 48 BDSG was an insufficient legal basis for the measure in question, the Hamburg Commissioner for Data Protection and Freedom of Information was able to deem the measure taken by the police illegal (for lack of a sufficient legal basis).[47]

And, indeed, Mysegades puts forwards reasons to doubt that Sec. 48 BDSG was a sufficient legal basis for the measures taken. He points out that the BVerfG in its decision on ALPR established criteria that would apply irrespective of whether an entire surveillance system is being established. Rather, specific aspects would have to be put into consideration, such as the (high and indeterminate) number of uninvolved persons being surveyed, the covert nature of the measure, and a feeling of citizens that they

[41] Here, the specific procedural facts of the case were also discussed. As the Hamburg Commissioner for Data Protection and Freedom of Information had issued an administrative act, the principle of the primacy of law came into play. The VG – obiter – expressed grave doubts whether the administrative act – as a decision by the executive branch for an individual case – could at all apply, as it might override statutory law, VG Hamburg, BeckRS 2019, 40195, paras 93 et seq.

[42] In this context, see Greve, '§ 48 BDSG', para. 21 on how Sec. 48 BDSG conforms with the constitution.

[43] VG Hamburg, BeckRS 2019, 40195, para. 101.

[44] Ibid., para. 102–103.

[45] Mysegades, 'Keine staatliche Gesichtserkennung', p. 852. On Sec. 48 (1) BDSG and FRT, see also Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', pp. 9–10; Marion Albers and Anna Schimke, '§ 48 BDSG' in Heinrich Amadeus Wolff and Stefan Brink (eds.), *BeckOK Datenschutzrecht* (42nd ed., CH Beck, 2022), paras 11–12; Frank Braun, '§ 48 BDSG' in Peter Gola and Dirk Heckmann (eds.), *DS-GVO/BDSG* (3rd ed., CH Beck, 2022), para. 10; Florian Albrecht, '§ 32 NPOG' in Markus Möstl and Bernhard Weiner (eds.), *BeckOK Polizei- und Ordnungsrecht Niedersachsen* (25th ed., CH Beck, 2022), para. 14b; Moritz Votteler, '48 BDSG' in Andreas Decker, Johann Bader and Peter Kothe (eds.), *BeckOK Migrations- und Integrationsrecht* (13th ed., CH Beck, 2022), para. 5.

[46] Cf. Greve, § 48 BDSG, para. 21.

[47] Mysegades, 'Keine staatliche Gesichtserkennung', pp. 852–853.

https://doi.org/10.1017/9781009321211.016 Published online by Cambridge University Press

were being monitored, which might flow from the broad ambit of the measure taken.[48] In particular, Mysegades contests an argument of the VG regarding the societal impact of the measures. While the VG argued that only those bystanders were being subjected to surveillance and further scrutiny who had willingly gone to the places where riots took place, Mysegades points out that Article 8 (1) GG protects the freedom to assemble, and that this freedom is infringed upon if future participants of assemblies feel the chilling effect of potentially being affected by FRT if they partake in assemblies.[49]

Moreover, Mysegades emphasises that when drafting Sec. 48 BDSG, the legislator had no intention for it to apply to FRT. When the provision was passed, the pilot study at Berlin Südkreuz (see Section 13.3.1) was already under way. Thus, it stands to reason that the legislator could and would have created a more specific provision for the highly contentious and sensitive issue of FRT use.[50]

Additionally, in its analysis of whether the measure was 'absolutely necessary', the VG refers to the necessity of automatic recognition measures for search sweeps within the data collected. Mysegades points out two issues with this approach.[51] The VG in its judgment does not provide a legal basis for all the individual steps of data processing and data collection. This also affects the court's analysis of whether the measure was absolutely necessary. The court held that automatic data processing was absolutely necessary, as processing the data collected by humans would not have been possible within a reasonable time frame. With this approach, the necessity of data processing is being linked to the data collected in the first step. However, the judgment does not answer whether and on what legal basis the data collection itself was justified.[52] One might expect such discussion to be linked to an over-arching goal of the measure, such as prosecution (or, in other scenarios, prevention) of crime.[53]

Lastly, the court could also have considered and given more weight to further risks for citizens' rights, such as potential abuse of the data collected, and, at the same time, the long period of time during which data was possibly stored.[54]

13.3.3 *Use of FRT for a Limited Time and with Specific Cause in the City of Görlitz*

The third and final example concerns the use of FRT for a specific purpose: FRT is being used in Görlitz, the easternmost city in Germany, located near the Polish and Czech borders. Since 2019, FRT cameras have been used there to combat serious

[48] Ibid., p. 854.
[49] Ibid.
[50] Ibid.
[51] Ibid., p. 855.
[52] See also Braun, '§ 48 BDSG', para. 10: the decision 'shows how not to' assess whether a measure was 'absolutely necessary'.
[53] On the background of the provision and for more details on the test whether a measure is absolutely necessary, see Greve, '§ 48 BDSG', para. 15.
[54] Mysegades, 'Keine staatliche Gesichtserkennung', p. 855.

border crime.[55] Görlitz is part of a corridor that is under video surveillance for a distance of 30 km. This use of FRT technology is aimed at addressing severe crimes and enhancing security in the area.

This application of FRT has its legal foundation in Section 59 Gesetz über die Aufgaben, Befugnisse, Datenverarbeitung und Organisation des Polizeivollzugsdienstes im Freistaat Sachsen (Law on the Tasks, Powers, Data Processing and Organisation of the Police Enforcement Service in the Free State of Saxony – SächsPVDG)[56]:

> Use of technical means to prevent severe cross-border crime
> (1) The police may, in order to prevent cross-border crime [as enumerated] collect personal data by the open use of technical means to make image recordings of traffic on public roads and to record information on the place, time and direction of use in order to compare it automatically with other personal data. This applies to road sections in the border area with the Republic of Poland and the Czech Republic up to a depth of 30 kilometres, insofar as facts justify the assumption that the road section in question is of outstanding importance for cross-border crime because it is regularly used as a venue for the commission of criminal acts within the meaning of sentence 1 or for the transfer of property or assets resulting from these criminal acts. The outstanding importance for cross-border crime must be evident from facts documented by the police. Technical and organisational measures must be taken to ensure that such means are not used either individually or in combination on a widespread or continuous basis.
>
> (2) Personal data in the sense of paragraph 1 may only be further processed to the extent that it is automatically compared with personal data of specific persons who are under police surveillance for the prevention of criminal offences within the meaning of paragraph 1 sentence 1.
>
> The data collected has to be deleted by automated means after ninety-six hours at the latest, unless the automated comparison revealed a match, and the data are required for the prevention or prosecution of criminal offences within the meaning of paragraph 1 sentence 1.
>
> (3) Measures pursuant to paragraph 1, including the determination of those persons whose data are absolutely necessary for [their] identification are to be processed for automated comparison, may only be ordered by the President of the State Criminal Police Office (Landeskriminalamt) or of a Police Directorate or by an official commissioned by them for this purpose. At the latest after the expiry of six months, the ordering police station shall check whether the conditions for the order still exist. The result of the examination has to be documented. The basis for the decision, including the findings in accordance with paragraph 1 sentence 3, which led to the respective operation, have to be documented for each measure.

[55] Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', p. 11.
[56] For a discussion of this provision, see in particular ibid., pp. 11–13, which also addresses concerns with regard to Art. 10 JHA Directive.

> (4) The necessity, practical application, and effects of the provisions of paragraphs 1 to 3 have to be examined by the state government. The state government has to report to the Landtag on the result of the evaluation three years after this Act comes into force.[57]

This provision has been drafted specifically for FRT measures.[58] Section 59 SächsPVDG allows the collection and recording of data (image recordings) to compare them automatically with other personal data. This provision, therefore, addresses many of the issues raised by the BVerfG and in the discussion of the measures by the police after the G20 riots. In contrast with Section 48 (1) BDSG, this provision is written in more detail and thus appears less problematic as a basis for FRT measures.

In the first place, the provision clearly states its purpose – it is directed at the prevention of grave cross-border crime. Pertinent crimes are explicitly enumerated in paragraph 1 sentence 1 and include human trafficking, gang theft, robbery, and severe cases of drug trafficking.

To conform with the ban on total surveillance,[59] technical and organisational measures must be put in place to ensure that such means are not used either individually or in combination on a widespread or continuous basis (paragraph 1 sentence 4).

As regards proportionality in a narrower sense,[60] it appears particularly relevant that the provision clearly states and restricts its geographic scope to road sections in the border area, that is with the Republic of Poland and the Czech Republic up to a depth of 30 kilometres.[61] Furthermore, concrete facts documented by the police must justify the assumption that the road section in question is of outstanding importance for cross-border crime, and according to paragraph 1 sentence 4, organisational measures must guarantee FRT is not applied on a widespread basis. However, Martini points out two regards in which this provision may not be sufficiently determinate in view of the requirement of legal certainty: it may not be sufficiently clear (1) when a road section is of outstanding importance for cross-border crime and (2) how far 'road sections' extend.[62]

The use of FRT is also limited in further respects. There is a time limit on the storage of data, and personal data may only be further processed to the extent that it is automatically compared with the personal data of specific persons who are already under surveillance for enumerated crimes. The data collected shall be deleted by automated means after ninety-six hours *at the latest*. If FRT procedures can be completed in a shorter time, the wording 'at the latest' may be viewed as a further guarantee of proportionality, requiring an earlier deletion where possible.

[57] Translation by the author.
[58] Sächsischer Landtag, Drucksache (LT-Drs) 6/14791, p. 186; Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', p. 11.
[59] See BVerfGE 125, 260, 324, para. 218.
[60] Cf. BVerfGE 150, 244, para. 90.
[61] Cf. Martini, 'Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit', p. 12.
[62] Ibid.

Section 59 (3) includes further procedural safeguards. Measures have to be based on a specific order and may only be ordered by the President of the State Criminal Police Office or of a police directorate or by an official commissioned, and have to be re-assessed as to whether the conditions for the order still exist (sentence 2). As a further procedural safeguard, the factual basis for this decision and pertinent findings by the police *shall be documented for each measure*. Again, potential criticism might be directed at the maximum period of six months for a re-assessment of the measure, but the wording 'at the latest' allows for a shorter period. Martini argues that further safeguards might be needed concerning supervision and transparency, and in particular, given the gravity of FRT, a decision by a court (instead of a member of the executive) might be in order.[63]

13.4 CONCLUSION

So far, FRT has only been employed in individual cases in Germany. The BVerfG has acknowledged that a ban on total surveillance is part of Germany's constitutional identity. For individual measures, constitutional key considerations concern their proportionality, the clarity of legal rules, and certainty. Furthermore, specific procedural safeguards are required.

This arguably amounts to a high threshold for FRT measures, as the examples discussed show. The permanent use of FRT without specific cause cannot be based on the existing provision Section 27, sentence 1 no. 2 BPolG, as it is not sufficiently specific. The use of FRT for analysis of video recordings from mass gatherings (as after the G20 riots) based on Section 48 (1) BDSG was viewed in a positive light by an administrative court. However, commentators raise the issues of legal clarity and certainty, and point out that the administrative court has not sufficiently explained the proportionality of the measures in this instance. Finally, even a very specific provision on the use of FRT for a limited time and with specific cause has been criticised for a potential lack of proportionality and for not being specifically determinate in certain regards.

[63] Ibid., p. 12.

https://doi.org/10.1017/9781009321211.016 Published online by Cambridge University Press