Diffusion of responsibility through the use of algorithms and AI in the area of internal security – allocation of responsibility through (constitutional) law?

Michael Bäuerle

The article examines the phenomenon of the diffusion of responsibility through algorithms from a constitutional law perspective using the example of the security authorities.

A. Scope and delimitation

Security authorities[1] like police, customs and intelligence services use increasingly systems controlled by algorithms and artificial intelligence. Techniques such as automatic facial recognition, automatic license plate reading systems, crime prediction systems, automatic data analysis and forensic evaluation of mobile phones and personal computers now regularly complement the general information and communication technologies that has long been used by the security authorities.[2] Algorithms and AI in the hands of security authorities now monitor and recognize people, extract "new knowledge"[3] from existing data sets and make predictions about when and where crimes will be committed. This gives the task fulfilment of security authorities new dimensions.

1 Agencies whose most important task is to maintain internal security. Cf. to the legal-political concept of internal security in Germany the Standing Conference of Federal and State Interior Ministers/Senators, Program for Internal Security in the Federal Republic of Germany, Part I, June 1972, Supplement to GMBl. No. 31/1972, Preliminary Remarks (p. 5): "Internal security is a central issue in contemporary politics. It is primarily about protecting the individual from crime, but increasingly also about protecting the institutions of the state and its basic democratic order." An addition to the program was made in 1974, supplement to GMBl. no. 9/1974.

2 See also Bäuerle, CRi 2022, 33 ff. with the in-depth distinction between general and task-specific use of information and communication technology by the security authorities.

3 See BVerfG NVwZ 2023, 1169 (1201, para. 67).

Although Security authorities do not yet make exclusively automated decisions within the meaning of Art. 11 Directive (EU) 2016/680[4] or fully automated administrative acts within the meaning of Section 35a VwVfG,[5] the use of the mentioned algorithmically and/or AI-controlled Systems and tools leads - depending on the result - to further intervention measures, such as searches, seizures and confiscations, surveillance measures, the use of undercover investigators, telecommunication surveillance and/or arrests or detentions.

If such measures take place due to algorithmically and AI-controlled processes, this means diffusion of responsibility to the extent that the underlying facts or the selected target persons were identified or selected automatically and not by an official, therefore not under the responsibility of the acting officials. In view of the lack of traceability[6] and the susceptibility to error and discrimination[7] of algorithmically or AI-controlled processes, the question of the allocation of responsibility arises when police interventions in fundamental rights are carried out on the basis of the results of such processes.

The following article examines the resulting legal questions primarily from a constitutional perspective. From this perspective, the "algorithmic turn"[8] among the security authorities is embedded in a long history of legis-

4 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, implemented inter alia by Part III of the BDSG and corresponding sections in the data protection laws of the federal states. In accordance with the area exception in Art. 2 para. 2 d) GDPR, this does not apply to this area, which also includes the protection against and the prevention of threats to public security in accordance with Art. 1 para. 1 Directive (EU) 2016/680. However, a provision corresponding to the content of Art. 11 Directive (EU) 2016/680 can also be found in Art. 22 GDPR.

5 In the USA, however, technologies that come close to exclusively automated decisions are already being used for security and law enforcement, see Rückert, *Mit künstlicher Intelligenz auf Verbrecherjagd: Einsatz von Gesichtserkennungstechnologie zur Aufklärung der "Kapitolverbrechen", VerfBlog,* 2021/1/22, https://verfassungsblog.de/ki-verbrecherjagd/ (accessed on 28.4.2024).

6 See Martini, Blackbox Algorithmus, 2019, p. 88 ff.

7 See Fröhlich/Spiecker genannt Döhmann: *Können Algorithmen diskriminieren?, VerfBlog,* 2018/12/26, https://verfassungsblog.de/koennen-algorithmen-diskriminieren/ (accessed 28.4.2024).

8 Term used by Sommerer, Predictive Policing, 2020, p. 260 (here in relation to crime control).

lative expansion of their informational powers and the constant correction of this development by the Federal Constitutional Court.

As a result, the German legal system proves to be well equipped to counteract the diffusion of responsibility through algorithms in the area of security authorities.[9]

B. Legal-political and social Background

The law governing security authorities in Germany has been undergoing dynamic change for some time.[10] The context for this development was initially formed by changes to the so-called security architecture,[11] ongoing legislative adjustments and their continuous "monitoring" by the Constitutional Court.

9 Not covered in the interest of limiting the subject matter of the study is the Europeanization that occurred recently to informational powers of security agencies, see e.g. Title V of the TFEU (Art. 67 to 89) and Art. 16 Abs. 2 TFEU and the European legislation based on it like Data Protection Directive for police and justice (Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119 p. 89, as amended in 2018 L 127 p. 9 and 2021 L 74 p. 36); See on this development Aden, HdB Polizeirecht, Section M, para. 1 et seq. with further references; for criticism, see Pfeffer, Vom Verfassungsstaat zur Sicherheitsunion, p. 75 ff.

10 For example Wolff/Brink, BeckOK DatenschutzR/Albers, Vorb. Syst. L., para. 1 ("few areas have changed so much in recent decades"), Löffelmann, GSZ 2021, p. 16 ("conspicuous reform dynamics"); Bäcker, Kriminalpräventionsrecht, 2015, p. 1 f. (characterizing the "permanent reform" of security law as a symptom of the "regulatory crisis of public law").

11 For more details, see Bäcker in Herdegen/Masing/Poscher/Gärditz, VerfassungsR-HdB § 28, para. 5 et seq.

I. Expansion of the tasks of the security authorities and technological change

In the face of new threats to state and society, the security authorities - namely the federal and state police forces and intelligence authorities[12] - were initially centralized, expanded[13] and their areas of responsibility extended.[14]

As a result of the legally created "preliminary tasks"[15] of the security authorities, their concepts of action developed from a reactive case-by-case approach to a (also) structure-oriented "operational" approach.[16] The more it became necessary to recognize security risks for civil society at an early stage and to ward them off in a promising manner, the more the authorities were dependent on the acquisition and processing of information; only when sufficient information is available on the state side can corresponding

12 In the following, the examination is essentially limited to these authorities, as their traditional main tasks - the prevention of threats to public security and the investigation of efforts against the free democratic basic order - outline the area that is referred to in the political arena as internal security. In the interest of limiting the subject matter of the investigation, the authorities entrusted with foreign or military-specific tasks (Federal Intelligence Service and Military Counterintelligence Service) are therefore excluded, unless there is case law from the Federal Constitutional Court relevant to the topic.
The regulatory and administrative authorities, which in many federal states are also responsible for averting danger (cf. for example § 1 Para. 1 HSOG, § 1 Para. 1 Rh.-Pf. POG), are still not considered, since public security is only one responsibility among others.

13 For more details, see Wolff/Brink, BeckOK DatenschutzR/Albers, Vorb. Syst. L., para. 5 et seq.

14 In the case of intelligence authorities, the traditional task of monitoring anti-constitutional efforts was (partially) extended to terrorism and/or organized crime (see Möstl/Schwabenbauer, BeckOK PolR Bayern/ Lindner/Unterreitmeier, Syst. Vorb., para. 1 ff.); in the case of the police authorities, the traditional task of averting danger was extended to include the task of preventively combating criminal offences (see Lisken/Denninger PolR-HdB/Denninger, Section B, para. 14 ff.).

15 On the term instead of many Möstl/Schwabenbauer, BeckOK PolR Bayern/Möstl, Syst. Vorb. PolR Deutschl., para. 43 ff. with further references; what is meant is that action may already be taken before the traditional police and criminal procedure law intervention thresholds of concrete danger to public safety or order or suspicion of a criminal offense are exceeded.

16 See Bäcker, HdB VerfR, § 28, para. 18 ff., 23 ff.

danger and suspicion hypotheses be created, checked and made the basis for suitable measures.[17]

This development coincided with the technological change in information technology, which resulted, among other things, in the far-reaching datafication of social communication.[18] This change not only created new (potential) sources of information for the security authorities, but also instruments and technologies for their exploitation and analysis as well as the generation of knowledge as such.[19] Those instruments and technologies include regularly algorithmically and AI-controlled processes, which causes the diffusion of responsibility described above.

II. Intensification of information-related legislation

The expansion of tasks and technological change in turn necessitated an adaptation and expansion of the legal basis for the collection and use of data and information by the security authorities. The increasing pace of federal and state legislative activity, particularly from the beginning of the 2000s,[20] resulted in a disproportionate increase in the information-related part of security legislation.

For example, in the Hessian Law on Public Security and Order (HSOG), only 30 of its 129 paragraphs - i.e. around 23% - currently refer to the handling of data, but their text comprises more than 49% of the entire legal text; in the Bavarian Police Duties Act (BayPAG), the data-related provisions account for around 33% (34 of 102 paragraphs), but make up around 63% of the entire legal text.[21] It is therefore correctly diagnosed in the literature that "the law governing the police and intelligence services

17 Lisken/Denninger PolR-HdB/Müller/Schwabenbauer, Section G, para. 2; Altwicker, p. 100, is also succinct: "Precautionary measures taken in advance of the danger are primarily information management."

18 Wolff/Brink, BeckOK DatenschutzR/Albers, Vorb. Syst. L., para. 1.

19 Wolff/Brink, BeckOK DatenschutzR/Albers, Vorb. Syst. L., para. 1, referring, among others, to the increasing use of artificial intelligence.

20 This can be seen, for example, in the list of amendments to the Code of Criminal Procedure in the large number of changes made between 1992 and 2022 in Section 8 of Book 1 ("Investigative measures", Sections 94 to 111q).

21 Numbers calculated using the word and character counting function in Microsoft Word.

is now to a large extent the law governing the handling of personal information and data."[22]

III. The Federal Constitutional Court as a permanent corrective

The expansion of the security authorities' informational powers has proven to be just as constant as its review by the constitutional court. "We know," says *Volkmann*, "that every new regulation in the area of security that is introduced by the federal or state legislature is bound to end up before the BVerfG."[23]

In fact, in view of the Federal Constitutional Court's case law on the security authorities' informational powers - which is probably unprecedented in terms of the number and depth of its decisions for a single area of regulation - it is not difficult to speak of a constitutionalization of this area of law.[24]

C. Constitutionalization of the security authorities' informational powers

The finding of a constitutionalization of the security authorities' informational powers raises the question of why such comprehensive constitutional court control of legislative activity has occurred in this area of law in particular. This process, which has been subject to significant criticism in the legal literature,[25] can essentially be traced back to two constitutional starting points.

The review of information collected by the security authorities found its material basis early on in the constitutional court's understanding of the

22 Wolff/Brink, BeckOK DatenschutzR/Albers, Vorb. Syst. L., para. 2; Lisken/Denninger PolR-HdB/Müller/Schwabenbauer, Section G, Part I., para. 2 ("Teilgebiet des Informationsverwaltungsrechts"), Bäcker, HdB VerfR, § 28, para. 42, refers to the constantly expanding legal basis for the security authorities' information system; Gärditz, GSZ 2017, 1 (4) emphasizes the "key position" of the handling of data and information in security law.

23 Volkmann, NVwZ 2021, 1408 (1409).

24 For example, Möstl/Schwabenbauer, BeckOK PolR Bayern/Lindner/Unterreitmeier, BayVSG, Syst. Vorb., Heading IV vor para. 14 ff., Wolff, DVBl. 2015, 1076 (1078 ff.), Gärditz, GSZ 2017, 1 (3 f.); Schoch, VVDStRL 81 (2022), Aussprache und Schlussworte, p. 504, speaks of an "over-constitutionalization of security administrative law".

25 For example, von Gärditz, EuGRZ 2018, 6 (21 f.); Lindner/Unterreitmeier, DÖV 2017, 90 (93); Möstl, DVBl. 2010, p. 808 et seq.

fundamental right to free development of the personality guaranteed by Article 2 (1) of the Basic Law.

I. State handling of data as an encroachment on fundamental rights

According to the Federal Constitutional Court, this fundamental right supplements the special ("named") civil liberties as an "unnamed" civil liberty right, which - such as the privacy of correspondence, post and telecommunications and the inviolability of the home - also safeguard constituent elements of personality.[26] Its task is to guarantee the narrower personal sphere of life and the preservation of its basic conditions in the sense of human dignity as the supreme constitutional principle, which cannot be conclusively covered by the traditional concrete guarantees of freedom; this necessity exists in particular in view of modern developments and the new threats to the protection of the human personality associated with them.[27]

The court then recognized such new threats as early as 1983 in modern data processing; under these conditions, the general right of personality also guarantees the right of the individual to determine the disclosure and use of their personal data (right to informational self-determination), the court ruled in the so-called census judgment.[28]

This established that the informational activities of the security authorities, insofar as they concern personal data, must always be considered to have the quality of an encroachment on fundamental rights.[29] Since

26 See only BVerfGE 54, 148 (153) = NJW 1980, 2070. The case law of the Federal Constitutional Court is cited below from the official collection of decisions, insofar as it is published there; parallel references are only cited in the first citation and only for decisions that are not listed in the list in the appendix, in which parallel references are named.

27 BVerfGE 54, 148 (153); BVerfGE 65, 1 (41) = NJW 1984, 419 (421); also Di Fabio, Dürig/Herzog/Scholz, GG, Art. 2 para. 1, para. 127, on the openness to development of the general right of personality for the protection against actual or presumed new threats due to social or technical developments.

28 BVerfGE 65, 1 (41 and Ls. 1 and 2) with reference to and continuation of BVerfGE 54, 148 (155), BVerfGE 27, 1 (6) = NJW 1969, 1707; BVerfGE 27, 344, (350 f.) = NJW 1970, 555; BVerfGE 32, 373 (379) = NJW 1972, 1123; BVerfGE 35, 202 (220) = NJW 1973, 1226; BVerfGE 44, 353 (372 f.) = NJW 1977, 1489 and BVerfGE 56, 37 (41 ff.) = NJW 1981, 1431; BVerfGE 63, 131 (142 f.) = NJW 1983, 1179.

29 Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, 2002, p. 209 et seq.; Mann/Fontana, JA 2013, 734 (736); Bäcker in Herdegen/Masing/Poscher/Gärditz, VerfassungsR-HdB § 28, para. 2 et seq. with footnote 5; "the census judg-

then, restrictions on this right have only been permissible in the overriding public interest and on the basis of a sector-specific and sufficiently specific legal basis.[30]

II. Case law of the Federal Constitutional Court

The census ruling opened in cooperation with some procedural peculiarities for the admissibility of corresponding constitutional complaints the space for the court to comprehensively specify the constitutional requirements for informational authorizations of the security authorities.

1. Differentiated fundamental rights protection of privacy as a starting point

The court differentiated the constitutional requirements for informational authorizations of the security authorities based on the fundamental right affected by the respective authorization.[31] The protection of the privacy affected by such authorizations is guaranteed in the Basic Law with the secrecy of correspondence, post and telecommunications (Art. 10 GG),[32] the inviolability of the home (Art. 13 GG),[33] the general right of personality and the right to informational self-determination[34] as its manifestation through several special fundamental rights.[35] In 2008, the court developed the latter further again with a view to technological progress and the change in living conditions: the widespread use of information technology systems and their central importance for the individual lives of many people requires the protection of the general right of personality to be extended to the confidentiality and integrity of information technology systems.[36]

---

ment, which was not issued directly on security law, was also momentous"); Lisken/Denninger PolR-HdB/Schwabenbauer, Section G, para. 13 et seq.

30 BVerfGE 65, 1 (41 and Ls. 1 and 2).

31 See also Lisken/Denninger PolR-HdB/Schwabenbauer, Section G, para. 62 et seq.

32 For example in BVerfGE 100, 313 et seq.; BVerfGE 113, 348 et seq.; BVerfGE 154, 152.

33 Above all in BVerfGE 109, 279 et seq.

34 For example in BVerfGE 120, 378 et seq.; BVerfGE 141, 220 et seq.

35 The Charter of Fundamental Rights of the European Union, which concentrates this protection in Art. 7 (respect for private and family life) and Art. 8 (protection of personal data), is different.

36 BVerfGE 120, 274 et seq. (online searches under the North Rhine-Westphalia Constitution Protection Act).

In the early rulings on the informational powers of the security authorities, it was primarily the secrecy of correspondence, post and telecommunications (Art. 10 GG)[37] and the inviolability of the home (Art. 13 GG)[38] that initially formed the fundamental rights benchmark. From the mid-2000s, the right to informational self-determination and then also the right to confidentiality and integrity of information technology systems came to the fore.[39]

Although all decisions related to authorizations for covert informational measures by security authorities, they can initially be read primarily as decisions on the special requirements for a specific informational interference with the respective fundamental right, which were also determined with regard to the specific tasks of the respective authorized authority.

However, with regard to the constitutional standards, the decisions show similarities from the outset with regard to the legal reservation under fundamental law and the principle of proportionality.

2. Legal reservation and proportionality as overarching standards

Uniform requirements initially result from the reservation of the law, which, according to the understanding of the court[40] , generally requires the legislator to regulate all essential questions - in particular those that are important for the realization of fundamental rights[41] - itself (so-called essentiality theory).

a) Sector-specific, sufficiently specific and sufficiently clear legal basis

In the census ruling, the court had already specified this for informational interventions to the effect that the basis for authorization must be formulated in a sector-specific manner and be sufficiently specific.[42] For covert in-

37 Thus in BVerfGE 100, 313 et seq.
38 BVerfGE 109, 279 et seq.
39 E.g. in BVerfGE 120, 378 et seq. and BVerfGE 120, 274 et seq.
40 See, for example, BVerfGE 40, 237 (249 with further references) = NJW 1976, 34; BVerfGE 49, 89 (126 f.) = NJW 1979, 359; BVerfGE 84, 212 (226) = NVwZ 1991, 1072; BVerfGE 83, 130 (142 ff.) = NJW 1991, 1471; BVerfGE 95, 267 (307 f.) = NJW 1997, 1975.
41 Only BVerfGE 47, 46 (80) = NJW 1978, 807; BVerfGE 49, 89 (127); BVerfGE 98, 218 (252 ff.) = NJW 1998, 2515.
42 BVerfGE 65, 1 (46).

formation interventions by the security authorities, the court now requires in particular that the reason, purpose and scope of the intervention be specified in concrete terms and clearly defined by law. In this respect, the authorization must be determined in such a way that the authorities addressed are guided and limited by the legal requirements and specifications ("intervention thresholds") and the potentially affected parties are put in a position to assess possible measures against them.[43] This is all the more important as legal protection in the case of covert security measures is regularly only available to a limited extent and the parliamentary and social control required by democratic theory is at least reduced in this area.[44]

Finally, the legal definition of the purpose of the measure is important in view of the principle of purpose limitation of data collection, which has also been in force across the board since the census ruling.[45]

b) Proportionality of the enabling provision(s)

In addition to these requirements, the Federal Constitutional Court also consistently instrumentalized the constitutional principle of proportionality[46] as an overarching standard of review for statutory authorizations of the security authorities to covertly interfere with information.[47] These had to be suitable, necessary (lack of a milder means) and appropriate (proportionality of purpose and means) for the intended purpose.[48] In this respect, it derived a whole bundle of formal and material requirements from the

43 BVerfGE 113, 348 (375 et seq.); BVerfGE 120, 378 (407 et seq.); BVerfGE 133, 277 (336); BVerfGE 141, 220 (265).

44 BVerfGE 113, 348 (375 et seq.); BVerfGE 120, 378 (408); BVerfGE 133, 277 (336 et seq.); BVerfGE 141, 220 (265); BVerfGE 155, 119 (177); BVerfGE 156, 11 (44 et seq.).

45 BVerfGE 65, 1 (47 et seq.) and then BVerfGE 100, 313 (360 et seq.); BVerfGE 109, 279 (375 et seq.); BVerfGE 110, 33 (73); BVerfGE 120, 351 (368 et seq.); BVerfGE 125, 260 (333); BVerfGE 130, 1 (33 et seq.); BVerfGE 133, 277 (372 et seq.); BVerfGE 141, 220 (324).

46 In general, for example, BVerfGE 50, 217 (227) = NJW 1979, 1345; BVerfGE 80, 103 (107) = NJW 1989, 1985; BVerfGE 99, 202 (212 ff.) = NJW 1989, 935, in more detail Grzeszick, Dürig/Herzog/Scholz, GG, Art. 20, para. 119 ff., on the literature's criticism of this standard, see the references ibid, para. 120, fn. 6.

47 For example, BVerfGE 120, 274 (318 f.); BVerfGE 125, 260 (316); BVerfGE 141, 220 (265), in each case with further references.

48 For more details, see Grzeszick, Dürig/Herzog/Scholz, GG, Art. 20, para. 114, 115 ff., 119 ff.

appropriateness - also referred to as proportionality in the narrower sense - which the legislators must meet.[49]

III. The constitutional requirements for information interventions by the security authorities in detail

On this basis, between 1999 and 2023, the court reviewed more than two dozen proceedings statutory authorizations of the security authorities to interfere with information, initially primarily challenging individual instruments - such as the "large-scale eavesdropping attack", preventive telecommunications surveillance or the use of license plate reading systems.[50] Later, constitutional complaints were added, in each of which a larger number of informational power norms from an entire body of law were put under scrutiny.[51]

While the principle of proportionality formed the central standard of review in the decisions, its standards varied - as a result of the need for a balancing of interests inherent in the criterion of appropriateness - according to the intensity of the encroachment on fundamental rights authorized by the provision under review. In this respect, the court successively developed criteria that can be used to determine the intensity of the encroachment of the security authorities' informational encroachment powers.

1. Criteria for determining the intensity of intervention

The court's explanations on the weight of the interference[52] initially revert to formulations that can already be found in the census judgment. The typical introductory sentence reads: "In general, the weight of an interference with informational self-determination is determined above all by the type, scope and conceivable use of the data as well as the risk of its misuse."[53]

---

49 For example, BVerfGE 141, 220 (265, 267 f., 290 f.) and the criticism of this in the dissenting opinions of Judges Eichberger (354 f.) and Schluckebier (365); see also BVerfGE 120, 274 (318 ff.); BVerfGE 125, 260 (316).

50 BVerfGE 109, 279 et seq.; BVerfGE 113, 348 et seq.; BVerfGE 120, 378 et seq.

51 E.g . in BVerfGE 141, 220 et seq. (BKA-G); BVerfG, NJW 2022, 1583 et seq. (Bayr. VerfassungsschutzG), BVerfG, GSZ 2032, 98 et seq. (PolizeiG M-V).

52 See also in detail Schwabenbauer, HdB Polizeirecht, Section G, para. 119 et seq.

53 BVerfGE 156, 11 (48 f.); BVerfG BeckRS 2023, 1828, para. 76 in each case with further references and with reference to BVerfGE 61, 1 (48 f.).

It is then regularly further stated that[54] it is important how many fundamental rights holders are exposed to how intensive impairments and under what conditions these occur, in particular whether these persons have given cause for this. The number of persons affected and the intensity of the individual impairment are therefore decisive. The weight of the individual impairment depends on whether the persons concerned remain anonymous, what personal information is collected and what disadvantages the holders of fundamental rights suffer as a result of the measures or fear without good reason. In particular, the secrecy of a state intervention measure leads to an increase in its intensity, as does the de facto denial of prior legal protection and the difficulty of obtaining subsequent legal protection, if such protection can be obtained at all.[55]

Based on these typical general findings of the court, the criteria used to determine the weight of the interference can ultimately be divided into qualitative, quantitative and modal criteria.[56]

From a qualitative perspective, the affiliation or proximity of the (potential) information to be collected or used to the privacy[57] of the data subjects plays a role. The more deeply the collection and/or processing of information by the security authorities interferes with this sphere, i.e. the space in which the individual is usually left to his or her own devices unobserved, the greater the weight of the interference.[58]

54 On the following BVerfGE 156, 11 (48 f.); BVerfG BeckRS 2023, 1828, para. 76; BVerfGE 100, 313 (376); BVerfGE 115, 320 (353); BVerfGE 141, 220 (265), in each case with further references.

55 See previous footnote for evidence.

56 However, it is not possible to draw a clear-cut distinction between these three groups; the subdivision in Lisken/Denninger PolR-HdB/Schwabenbauer, Section G, para. 119 et seq. differs somewhat.

57 According to the BVerfG, the private sphere has always been part of the scope of protection of the general right of personality, see for example BVerfGE 90, 255 (260) = NJW 1995, 1015: "Such a sphere is established by the general right of personality. Art. 2 para. 1 GG guarantees the free development of personality. One of the conditions for the development of personality is that the individual has a space in which he is left to himself unobserved or can associate with persons of his particular trust without regard to social expectations of behavior and without fear of state sanctions. It follows from the importance of such a retreat for the development of the personality that the protection of Article 2.1 in conjunction with Article 1 of the Basic Law also includes the private sphere (see BVerfGE 27, 1 (6) = NJW 1969, 1707; established case law)".

58 See BVerfGE 100, 313 (358 et seq.); BVerfGE 107, 299 (312 et seq.); BVerfGE 110, 33 (52 et seq.); BVerfGE 113, 348 (364 et seq.); BVerfGE 115, 320 (341 et seq.); BVerfGE 125, 260 (316 et seq.); BVerfGE 133, 277 (335 et seq.); see also Lisken/Denninger PolR-HdB/Schwabenbauer, Section G, para 62, 111 et seq.

Since the protection of privacy extends in particular to confidential communications,[59] the potential inclusion of corresponding communication relationships in the collection and processing of information by the security authorities also increases the weight of interference.[60]

In quantitative terms, the number of persons potentially involved in the collection or processing of information by the security authorities ("range") is important for the intensity of the interference, as is the duration and intensity of the measure in relation to the individual persons concerned. The court[61] sees a wide range that increases the weight of the interference if numerous persons are included in the scope of a measure who have no connection to a specific misconduct and did not cause the interference through their behavior. Accordingly, the individual's fundamental freedom is affected all the more intensely the less they themselves have given rise to a state intervention.

Such interventions could also have an intimidating effect, which could lead to impairments in the exercise of fundamental rights.[62] A deterrent effect on the exercise of fundamental rights - according to the further justification - must not only be avoided in order to protect the subjective rights of the individuals concerned; the common good is also impaired because self-determination is an elementary functional condition of a free democratic community based on the ability of its citizens to act and participate.[63] It jeopardizes the impartiality of conduct if the wide range of investigative measures contributes to the risk of abuse and a feeling of being under surveillance.[64]

---

59 BVerfGE 90, 255 (260): "Confidential communication is also part of the protection of privacy. Particularly in the case of statements made to family members and persons of trust, the focus is often less on the aspect of expressing opinions and the intended influence on the opinion-forming of third parties than on the aspect of self-expression."

60 BVerfG, BeckRS 2022/41609, para. 102 (passage not reprinted in GSZ 2023, 98 et seq.); BVerfGE 141, 220 (276), on the resulting absolute restriction of the core area of private life, see cc) below.

61 For the first time in BVerfGE 100, 313 (376, 392), then for example in BVerfGE 107, 299 (320 f.); BVerfGE 109, 279 (353); BVerfGE 113, 29 (53); BVerfGE 113, 348 (383); see also Lisken/Denninger PolR-HdB/Schwabenbauer, Section G, para. 132.

62 This was already the case in the census judgment, BVerfGE 65, 1 (42), then BVerfGE 113, 29 (46).

63 BVerfGE 113, 29 (46).

64 BVerfGE 107, 299 (328); see also Lisken/Denninger PolR-HdB/Schwabenbauer, Section G, para. 125, 134.

In relation to the individual data subjects, the weight of the interference is also determined by the duration and scope of the respective monitoring measure. The longer the period of surveillance and the more comprehensively the movements and expressions of life of the person concerned are recorded, the more serious the intrusion.[65]

With regard to the modes of information collection, the covertness or secrecy of a measure per se increases the intensity of its intrusiveness.[66] Additional weight is added by the use of technical means, with the help of which perception hurdles are overcome or the processing of large complex data sets becomes possible.[67] The exploitation of trust worthy of protection in the identity and motivation of a communication partner also has an intrusive effect; finally,[68] the same applies to the risk or probability of being exposed to follow-up measures.[69]

2. Intervention intensity and need for regulation in the application of algorithm- or AI-controlled processes by the security authorities

On this basis, the court has recently also increasingly turned its attention to the use of algorithm- or AI-controlled processes in the context of data collection and data processing by the security authorities. Explicit statements on this can be found for the first time in a decision from 2020 on the strategic foreign telecommunications surveillance carried out by the Federal Intelligence Service, in which such processes played a decisive role, as foreign communications are automatically evaluated using certain search terms. On the question of which constitutional requirements the legal basis for this measure must meet, the court stated, among other things: "The framework provisions to be prescribed by law include the requirement of an immediate evaluation of the collected data (...), the application of the

65 BVerfGE 109, 279 (323); BVerfGE 112, 304 (319 f.); BVerfGE 130, 1 (24); BVerfGE 141, 220 (280 f.).

66 With regard to the collection of police information, BVerfGE 133, 277, 328 f.: "A secret police force is not envisaged."

67 BVerfG BeckRS 2023, 1828, para. 69 et seq.; BVerfGE 120, 274 (375); BVerfG NJW 2022, 1583 (1610).

68 In particular BVerfGE 120, 274 (375); BVerfG NJW 2022, 1583 (1610).

69 On the whole BVerfGE 107, 299 (318 et seq.); BVerfGE 109, 279 (353 et seq.); BVerfGE 113, 348 (382 et seq.); BVerfGE 115, 320 (347 et seq.); BVerfGE 118, 168 (169 et seq.); BVerfGE 120, 274 (322 et seq.); BVerfGE 125, 260 (318 et seq.); BVerfGE 141, 220 (268 et seq.).

principle of proportionality in the selection of search terms - as currently already provided for in the service regulations -, regulations on the use of intrusion-intensive methods of data evaluation, in particular complex forms of data comparison (...) as well as compliance with the prohibition of discrimination under the Basic Law (...). The use of algorithms may also need to be regulated, in particular to ensure their fundamental traceability with a view to independent control."[70]

The court expanded on this approach in a highly regarded decision on the use of the "Gotham"-program from Palantir Inc. by the Hessian police for the automated analysis of its own databases.[71] The program extracts correlations between people, groups of people, institutions, organizations, objects and things from police data, classifies incoming information according to known facts and evaluates the data statistically. It therefore generates "new knowledge" that could not otherwise have been derived from the data and presents this graphically in a form that is easy for users to understand.[72]

The court stated that the automated data analysis alone constitutes an interference with the right to informational self-determination and, in terms of the intensity of the interference, has an intrinsic weight that goes beyond that of the collection of the analysed data.[73] Depending on the complexity and "learning ability" of the algorithms used as well as the scope and sensitivity of the data involved, the use of such systems for automated data analysis is of the highest intensity of interference.[74]

As a result, the strictest requirements apply to legal authorizations for the use of such systems; the court had already differentiated these in its extensive case law.[75]

In particular, the requirements relate to thresholds of interference, protected interests and addressees of the measures, allow only limited exceptions to the purpose limitation of data and place high demands on the exchange of data between different authorities, in particular between the

70 BVerfG NJW 2020, 2235 (2253, para. 192).

71 BVerfG NJW 2023, 1196 ff., the decision concerned not only the legal basis created for data analysis in Hesse but also the parallel standard from Hamburg.

72 See BVerfG NJW 2023, 1196 (1201, para. 96 et seq.).

73 See BVerfG NJW 2023, 1196 (1201, para. 67 et seq.).

74 See BVerfG NJW 2023, 1196 (1201, para. 75 et seq.).

75 Cf. for example BVerfGE 100, 313 (360 f., 389 et seq.); BVerfGE 109, 279 (375 et seq.); BVerfGE 110, 33 (73); BVerfGE 120, 351 (368 et seq.); BVerfGE 125, 260 (333); BVerfGE 130, 1 (33 et seq.); BVerfGE 133, 277 (372 et seq.); BVerfGE 141, 220 (324); see also Lisken/Denninger PolR-HdB/Schwabenbauer, Section G, para. 23, 120, 222 et seq.

police and intelligence services. Furthermore, legal requirements for (prior) control, procedures, transparency and legal protection must be guaranteed and a core area of private life must always remain free from information interventions by the security authorities.

With regard to the specific system, legal specifications must also be made to reduce the risks of discrimination associated with automated data analysis and to counteract the susceptibility of the data analysis system to errors. If - as is the case here - the system of a private provider is used, government monitoring of the (further) development of the software must also be provided for.[76]

D. (No) diffusion of responsibility through algorithms under the conditions of the constitutionalization of the security authorities' informational powers

If we look at the constitutional requirements from the point of view of the court regarding the diffusion of responsibility through algorithms, it should first be noted that the Federal Constitutional Court primarily assigns responsibility for the use of AI and algorithm-controlled processes by the security authorities to the legislator.

Although the legislator may permit the use of such systems, it must counteract the risk of a diffusion of responsibility by making provisions to minimize the risks of discrimination and the susceptibility of AI or algorithm-controlled systems to errors. Furthermore, the typical risk of the non-traceability of algorithmically generated results must be limited by specifying transparency, procedures and controls and ensuring that legal protection can be obtained at any time in the event that errors nevertheless occur.

The fundamental rights of those affected must also be taken into account by restricting the data that may be used in AI and algorithm-driven analyses and by imposing restrictions on the technologies used, which - if they originate from state providers - also require state monitoring.

In the field of legal policy, technologies such as predictive policing or AI-supported surveillance of public spaces are often associated with dystopias that are easy to understand in view of the potential of such technologies for ubiquitous total surveillance. In the German legal system, these dystopias

76 BVerfG NJW 2023, 1196 (1202 et seq. para 77; 1204 et seq. para 95; 1205 Para 100; 1202 et para 109).

are unlikely to be based on a realistic prognosis under the conditions of the constitutionalization of the security authorities' powers of informational intervention.

Even if the risk remains that serious police or secret service measures may be taken in individual cases on the basis of faulty AI or algorithm-controlled processes, this should be readily acceptable in view of the potential associated with such technologies to make public security measures more effective as a result of the guarantee of subsequent control and correction.