Bavarian Protection of the Constitution Act unconstitutional in part

Press Release No. 33/2022 of 26 April 2022

Judgment of 26 April 2022
1 BvR 1619/17

In a judgment pronounced today, the First Senate of the Federal Constitutional Court found several provisions of the Bavarian Protection of the Constitution Act (*Bayerisches Verfassungschutzgesetz* – BayVSG) incompatible with the Basic Law (*Grundgesetz* – GG) because certain powers conferred upon the Bavarian domestic intelligence service, the *Land* Office for the Protection of the Constitution (*Landesamt für Verfassungsschutz*), violate fundamental rights. Some of the powers violate the general right of personality (Art. 2(1) GG in conjunction with Art. 1(1) GG) in its manifestation as the right to informational self-determination, some violate this right in its manifestation as the right to the confidentiality and integrity of information technology systems, while others violate the privacy of telecommunications (Art. 10(1) GG) and the inviolability of the home (Art. 13(1) GG).

a) Art. 9(1) first sentence BayVSG ("*surveillance of private homes*") is unconstitutional. While the power conferred thereunder requires in principle sufficient prerequisites for taking surveillance measures which constitute interference with fundamental rights ("acute danger", *dringende Gefahr*), it is not aimed at "averting" a danger to public security. The provision also lacks the necessary criterion of subsidiarity vis-à-vis public security measures taken by police authorities. Moreover, the constitutional requirements for the protection of the core of private life applicable to the surveillance of private homes are not fully met, either at the data collection stage or during the analysis of collected data.

b) Art. 10(1) BayVSG ("*remote searches*") is unconstitutional because that provision, by its reference to Art. 9(1) BayVSG, shares the same constitutional deficiencies. Although this provision meets the constitutional requirements for the protection of the core of private life at the data collection stage, it is deficient with respect to the analysis of collected data.

c) Art. 12(1) BayVSG ("*tracking of mobile devices*") is unconstitutional because the authorisation is so broad that it allows for long-term monitoring of the movements of the persons concerned (a "movement profile") without satisfying the applicable constitutional requirements. In this respect, the provision fails to provide for sufficiently specific prerequisites for interference and the necessary independent oversight.

d) Art. 15(3) BayVSG ("*disclosure of traffic data originating from data retention*") violates the principle of legal clarity.

e) Art. 18(1) BayVSG ("*undercover officers*") and Art. 19(1) BayVSG ("*informants*") are unconstitutional because they do not provide a sufficient threshold for interference and there is no restriction on the scope of permissible targets of surveillance if the use of undercover officers or informants is directed at specific persons. Moreover, the required independent oversight is lacking.

f) Art. 19a(1) BayVSG ("*observation outside the home*") is unconstitutional because in the case of particularly intrusive observations the authorisation is not limited to anti-constitutional endeavours or activities that particularly necessitate surveillance. Further, there is also a lack of independent oversight.

g) Insofar as the challenge to the data sharing provisions of Art. 25 BayVSG ("*data sharing by the Land Office*") is admissible, it is successful, as the provisions do not satisfy constitutional requirements. Some authorisations of data sharing are not aimed at protecting sufficiently weighty legal interests; some do not provide a sufficient threshold for data sharing. The powers of data processing and sharing under Art. 8b(2) first sentence no. 2 BayVSG *("data originating from the surveillance of private homes and remote searches*") are unconstitutional due to an impermissible dynamic reference to federal law. This also applies to Art. 8b(3) BayVSG ("*data originating from requests for information*"); further, the multi-level chains of statutory references contained in this provision violate the principle of legal clarity.

Art. 15(3) BayVSG is void. The rest of the provisions at issue are incompatible with the Basic Law but will continue to apply temporarily – subject to restrictions to protect the fundamental rights concerned – until 31 July 2023.

Facts of the case:

In 2016, the Bavarian Protection of the Constitution Act was revised and fundamentally restructured. The law distinguishes between general powers of information processing in Art. 5 BayVSG, the specific power to collect information by intelligence service means in Art. 8 BayVSG, and special intelligence service means, which are specifically set out in Art. 9 to Art. 19a BayVSG. Data sharing, including the sharing of personal data by the *Land* Office with other bodies, is generally set out in Art. 25 BayVSG. Art. 8b(2) BayVSG contains specific rules for the processing of personal data obtained through surveillance of private homes or through covert access to information technology systems. Art. 8b(3) BayVSG contains special requirements for the processing of personal data obtained through special requests for information pursuant to Art. 15(2) and (3) as well as Art. 16(1) BayVSG.

The complainants are members and, in some cases, active officials of organisations under surveillance by the Bavarian *Land* Office for the Protection of the Constitution and are also mentioned in its reports on the protection of the Constitution. They challenge various data collection and data sharing powers set out in the Bavarian Protection of the Constitution Act.

Key considerations of the Senate:

I. The constitutional complaint is ultimately directed against the surveillance powers of the Bavarian *Land* Office under Art. 9(1) first sentence, Art. 10(1), Art. 12(1), Art. 15(2) and (3), Art. 16(1), Art. 18(1), Art. 19(1), Art. 19a(1) and (3) first and fourth sentence, and its powers of data processing and sharing under Art. 8b(2) first sentence no. 2, and (3), and Art. 25(1) nos. 1 and 3, Art. 25(1a), Art. 25(2) first sentence nos. 2 and 3, Art. 25(2) second sentence, Art. 25(3) first sentence nos. 2 and 3 BayVSG. The constitutional complaint is inadmissible in part.

Insofar as the constitutional complaint is directed against surveillance powers, it is inadmissible with regard to the challenges to Art. 15(2) ("*information from postal service providers, telecommunications services and telemedia*") and Art. 16(1) BayVSG ("*further requests for information*"), as the complainants failed to sufficiently demonstrate standing in this regard. The remainder of the constitutional complaint is admissible. Insofar as further processing and surveillance powers are challenged, the complaint is also partially inadmissible. The challenge to data sharing with bodies in other European states permitted under Art. 25(1a) BayVSG is inadmissible to the extent that data is shared with non-public bodies, because the possibility of a violation of fundamental rights has not been sufficiently substantiated. The same applies to the duty to share information with public prosecution offices, police and other authorities under Art. 25(1) second sentence BayVSG and to the power to share information with non-public bodies conferred in Art. 25(3) first sentence no. 3 BayVSG. The challenges regarding the provisions on transparency and oversight provided for in the Bavarian Protection of the Constitution Act are also inadmissible. This concerns the objection to Art. 11(2) third sentence, Art. 17(2) first sentence, Art. 20(1) and Art. 23(1) first sentence and third sentence nos. 1 and 2 BayVSG.

II. To the extent that the constitutional complaint is admissible, it is for the most part well-founded.

1. In some respects, the fundamental rights at issue give rise to different requirements as to the actions of domestic intelligence services than as to corresponding actions by police authorities. On the one hand, the surveillance powers of domestic intelligence services are not generally required to be linked to the existence of a danger in the same sense as for police action. Instead, the legislator can provide for a threshold for interference with fundamental rights specific to the protection of the constitutional order ("requirement of a need for intelligence specific to the protection of the constitutional order"). On the other hand, the sharing of personal data and information by a domestic intelligence service with other bodies – at least if the data was collected by intelligence service means – requires, without exception, that the data sharing both serves to protect a particularly weighty legal interest and that the threshold for the data sharing also satisfies the criterion of a hypothetical recollection of the data ("principle of separation of police and intelligence data").

a) According to the applicable law, domestic intelligence services perform specific tasks of surveillance and intelligence gathering to protect exceptionally significant legal interests. They do not have operational follow-up powers as police authorities do. This justifies a modified threshold for their use of surveillance powers compared to the threshold required for police surveillance. The particular constitutional requirements that apply to the covert surveillance powers of a domestic intelligence service follow, above all, from the fundamental right at issue in each case and the principle of proportionality in the strict sense. In this respect, constitutional requirements exist with regard to the legal interest to be protected, the threshold for interference – i.e., the grounds for the surveillance – and the procedural details relating to the interference.

Measures that could lead to an extensive intrusion upon one's personality are subject to the same proportionality requirements as police surveillance. Other covert surveillance powers of a domestic intelligence service, however, do not have to be linked to the existence of a danger in the same sense as for police action. Rather, the requirement is that there is a sufficient need for surveillance specifically relating to the protection of the constitutional order. This requires that there are sufficient factual indications of an anti-constitutional endeavour that necessitates surveillance for the purpose

of protecting the constitutional order and that the surveillance measures to be undertaken in the particular case are necessary. The greater the intensity of the interference resulting from the surveillance measure, the more urgently the endeavour must necessitate surveillance. The legislator must set forth in a sufficiently specific and clear manner what level of need for surveillance is required in each case. Special requirements apply when the persons under surveillance are not themselves part of the endeavour at issue or otherwise acting in furtherance of the endeavour. Depending on the intensity of the interference resulting from the measure to be carried out, a prior review of the measure by an independent body may also be necessary.

b) The principle of proportionality in the strict sense also places special requirements on the data sharing powers of a domestic intelligence service. The sharing of personal data and information by domestic intelligence services with other bodies constitutes a separate interference with fundamental rights. If the data was collected by intelligence service means, the justification for the interference resulting from the sharing of such data must be assessed according to the standard of a hypothetical recollection of the data. Based on this standard, whether the receiving authority may receive such data depends upon whether, in that particular case, the receiving authority could have been permitted to collect the same data and information using comparably intrusive means as the original surveillance by the domestic intelligence service. Data sharing therefore must always serve to protect a particularly weighty legal interest. The requirements for the threshold for data sharing differ according to which body the data is transmitted.

aa) In the case of data sharing with a police authority, the data sharing must serve to protect a particularly weighty legal interest for which there is at least a sufficiently identifiable danger (*hinreichend konkretisierte Gefahr*).

bb) Data sharing with a prosecution authority can only be considered for the purpose of prosecuting particularly serious criminal offences and requires a suspicion based on specific facts that is supported by sufficiently concrete and tangible circumstances.

cc) Data sharing with other bodies is also only permissible to protect a particularly weighty legal interest. The constitutional requirements for the threshold for data sharing differ according to the intensity of the interference, which inter alia, depends on the operational follow-up powers of the receiving authority. Data sharing with a domestic intelligence agency is therefore possible if there are sufficient factual indications in that particular case that the information is necessary for surveillance of a specific action or group that necessitates observation by intelligence services.

dd) The requirements for data sharing carried out domestically also apply to data sharing with other states. In addition, the recipient state must handle the shared data in accordance with basic human rights and data protection standards, and such compliance must be ascertained accordingly.

c) A statutory authorisation for covert surveillance measures must also be sufficiently clear and specific. The principle of legal clarity sets limits to the use of chains of statutory references in legislation. Confusing, multi-level chains of statutory references are incompatible with fundamental rights requirements.

2. The challenged powers of the *Land* Office for the Protection of the Constitution are not fully compatible with the requirements of proportionality in the strict sense.

a) *Art. 9(1) BayVSG – surveillance of private homes*

Art. 9(1) first sentence BayVSG, which authorises the *Land* Office to engage in acoustic and visual surveillance of private homes, is unconstitutional. Art. 13(4) GG only allows the use of acoustic or visual surveillance of private homes to avert acute danger. The surveillance must be specifically aimed at "averting" the danger. Art. 9(1) first sentence BayVSG does not contain such a limitation. Given the constitutional requirement of a direct link between the surveillance measure and averting danger, it also follows that a domestic intelligence service may only be granted the power to conduct surveillance on a private home on a subsidiary basis, i.e., only in the event that suitable police assistance for the legal interest at risk cannot otherwise be timely obtained. Such a requirement is lacking in Art. 9(1) BayVSG.

Furthermore, the general provisions in Art. 8a(1) BayVSG for the protection of the core of private life do not fully satisfy the applicable constitutional requirements in the case of surveillance of a private home. At the data collection stage, there is a constitutional presumption in favour of the protection of privacy, which must be expressly incorporated in the statutory basis. Such presumption is missing in Art. 8a(1) BayVSG. Art. 8a(1) BayVSG also does not satisfy the constitutional requirements with regard to the analysis of collected data, because it does not ensure that all information originating from the surveillance is fully reviewed by an independent body with regard to its relevance to the core of private life prior to the *Land* Office obtaining access to the information.

b) *Art. 10(1) BayVSG – remote searches*

Art. 10(1) BayVSG, which authorises the *Land* Office to use technical means to remotely access information technology systems within the sphere of control of targets of surveillance and thereby retrieve and collect data (a so-called remote search), is incompatible with the fundamental right to the confidentiality and integrity of information technology systems

as a specific manifestation of the general right of personality (Art. 2(1) GG in conjunction with Art. 1(1) GG). A remote search is only permissible where at least an identifiable danger, within the meaning of police law, exists. The measures authorised under Art. 10(1) BayVSG are not limited to this purpose, given that the provision contains a statutory reference to the requirements of Art. 9(1) BayVSG. In addition, as is the case with the surveillance of private homes, a domestic intelligence service may only conduct remote searches on a subsidiary basis.

The general provisions for the protection of the core of private life in Art. 8a(1) BayVSG also do not fully correspond to the special requirements applicable to remote searches. At the data collection stage, the requirements in Art. 8a(1) first sentence and Art. 10(2) first sentence no. 3 BayVSG are constitutional. However, the provisions relating to the analysis of collected data are insufficient for the protection of the core of private life, because they do not ensure that all information originating from the surveillance is fully reviewed by an independent body with regard to its relevance to the core of private life prior to the domestic intelligence service obtaining access to the information.

c) *Art. 12(1) BayVSG – tracking of mobile devices*

Art. 12(1) BayVSG, which authorises the tracking of mobile devices, is unconstitutional. The provision does not contain sufficiently specific prerequisites for interference. Its wording does not preclude the creation of movement profiles of persons under surveillance. This would constitute a serious interference with fundamental rights. If the legislator wants to grant the *Land* Office such extensive powers, then the legislator must provide for a qualified threshold for interference specific to the protection of the constitutional order. The use of such powers would require a heightened need for surveillance and the domestic intelligence service would have to be provided statutory direction as to when such a need arises. Such statutory direction is lacking here. Because the surveillance powers may be used for longer-term monitoring, including the creation of a comprehensive movement profile, independent oversight is also required due to the potentially high intensity of the interference. Art. 12(1) BayVSG also fails to provide for such oversight.

d) *Art. 15(3) BayVSG – disclosure of traffic data originating from data retention*

Art. 15(3) BayVSG enables the access of data stored by service providers under data retention rules. This provision is not compatible with the principle of legal clarity and violates Art. 10(1) GG because it authorises the access of data in the absence of any obligation or authorisation on the part of the service providers to share such data with the *Land* Office under federal law.

e) *Art. 18(1) BayVSG – undercover officers*

Art. 18(1) BayVSG, which authorises the use of undercover officers, violates the fundamental right to informational self-determination because the threshold for interference is insufficient. In light of the potentially serious interference with fundamental rights that Art. 18(1) BayVSG authorises, the applicable general provisions of Art. 5(1) BayVSG, which allow, in particular, action based on the existence of mere factual indications of anti-constitutional endeavours or activities are not sufficient. The law does not contain any specific requirements as to permissible duration of the use of undercover officers, nor does it provide for a duration of their use that is proportionate to the severity of the danger of the activities under surveillance. In addition, the Basic Law imposes strict limits on targeted inclusion of third parties in surveillance measures by domestic intelligence services, but the law contains no limitation on the permissible targets of surveillance when the use of undercover officers is directed against specific persons. Art. 18 BayVSG is also unconstitutional insofar as it fails to provide for any independent oversight.

f) *Art. 19(1) BayVSG – informants*

Art. 19 BayVSG, which governs the use of informants, with reference to the requirements of Art. 18 BayVSG, also violates the fundamental right to informational self-determination. The use of informants is subject in principle to the same constitutional requirements regarding the applicable threshold for interference and permissible targets of surveillance as the use of undercover officers. These requirements are not satisfied. Here, too, a sufficient threshold for interference is lacking, as well as a limitation of the permissible targets of surveillance when the use of informants is directed against specific persons, and there is no independent oversight.

g) *Art. 19a(1) BayVSG – observation outside the home*

Art. 19a(1) BayVSG, which authorises the *Land* Office to observe a person covertly and systematically, including using technical means, for longer than 48 hours or on more than three days within a week, violates the fundamental right to informational self-determination. The threshold for interference under this provision is insufficient. According to Art. 19a(1) last half-sentence BayVSG, observation is only permitted when necessary for the surveillance of endeavours or activities of “considerable significance”. The requirement of a particularly heightened need for surveillance in the case of especially intrusive long-term observation, which follows from the principle of proportionality, and the basis for such need, are not sufficiently specified. The constitutionally required independent oversight is also missing here.

h) *Art. 25 BayVSG – data sharing by the Land Office*

Insofar as the challenge to Art. 25 BayVSG is admissible, the data sharing authorised thereby violates the right to informational self-determination. It does not meet the standard of the hypothetical recollection of the data.

aa) To the extent that Art. 25(1) no. 1 second alternative BayVSG permits data sharing with domestic bodies "for public security purposes", it does not establish sufficient statutory requirements for data sharing. As phrased, data sharing is not limited to the protection of particularly weighty legal interests; instead, any breach of the law can justify data sharing. In addition, the constitutionally required threshold for data sharing is lacking because the only requirement for such data sharing is that there are factual indications that the recipient needs the information. This does not satisfy the applicable constitutional requirements.

bb) Under certain conditions, Art. 25(1) no. 3 BayVSG authorises the *Land* Office to share information, including personal data, with any domestic public body if there are factual indications that the recipient requires the information for the performance of its assigned duties, provided that the recipient thereby is also acting for the protection of the free democratic basic order or must assess issues of public security or foreign interests. This authorisation does not adequately specify the legal interests to be protected, nor does it provide for a sufficient threshold for the sharing of data.

cc) Art. 25(1a) BayVSG, the challenge to which is admissible insofar as it concerns the authorisation of data sharing by the *Land* Office with public bodies in other European states, shares the same constitutional deficiencies of Art 25(1) because it refers to that section without restriction.

dd) Art. 25(2) first sentence BayVSG, which authorises data sharing with authorities with executive powers, is unconstitutional insofar as the challenge thereto is admissible. Art. 25(2) first sentence no. 2 BayVSG authorises data sharing to avert, prevent or prosecute considerable criminal offences. For all three alternatives, this authorisation falls short of the constitutional requirements. The same applies for first sentence no. 3.

ee) Art. 25(3) first sentence no. 2 BayVSG, which authorises data sharing with foreign public bodies, as well as supranational and international bodies, also fails to satisfy constitutional requirements. The law permits data sharing where mere factual indications exist that it is necessary to protect the recipient's significant security interests. This fails to set forth specific grounds for investigation, either in the context of police investigation or intelligence service work.

i) *Art. 8b(2) first sentence no. 2BayVSG – data originating from the surveillance of private homes and remote searches*

Art. 8b(2) first sentence no. 2 BayVSG, which provides for the conditions of further processing and sharing of data originating from the surveillance of private homes and remote searches, violates Art. 13 GG and the general right of personality in its manifestation as protection of the confidentiality and integrity of information technology systems. It does not satisfy the constitutional requirements regarding a dynamic statutory reference. The Basic Law only permits dynamic references to laws passed by a different legislative authority under strict conditions, particularly as regards provisions that authorise an interference with fundamental rights. They may be permissible if the laws referred to relate to a narrowly defined field, and their contents are already essentially certain. That is not the case, however, for the reference to § 100b(2) of the Code of Criminal Procedure (*Strafprozessordnung* – StPO).

j)*Art. 8b(3) BayVSG–data from requests for information*

Art. 8b(3) BayVSG, which authorises the further processing and sharing of personal data originating from requests for information pursuant to Art. 15(2) and (3) and Art. 16(1) BayVSG, violates the general right of personality in its manifestation as the right to informational self-determination, and in part violates Art. 10(1) GG. Art. 8b(3) BayVSG itself does not contain any provisions as to whether and under what conditions data obtained from a request may be used and shared, but instead refers entirely to the corresponding provision of § 4 of the Article 10 Act (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* – G 10-Gesetz). This dynamic reference to a law from another legislative authority is also impermissible because the provisions referred to do not relate to a narrowly defined field, such that their contents are already essentially certain. The reference here also violates the requirement of legal clarity because the references exceed the constitutionally permissible limit of multi-link chains of reference.