Headnotes

to the Order of the First Senate of 8 June 2021

- 1 BvR 2771/18 -

(IT security vulnerabilities)

1. **Art. 10(1) of the Basic Law not only gives rise to a defensive right of the individual against state interference, but also requires the state to protect individuals from private third parties gaining access to communications that are protected by the privacy of telecommunications (confirming BVerfGE 106, 28 <37>).**

2. **a) The protection of the confidentiality and integrity of information technology systems, as guaranteed by fundamental rights, obliges the state to help protect such systems from attacks by third parties.**

   b) The state's duty of protection arising from fundamental rights also requires a legal framework that governs how – in a manner compatible with fundamental rights – the state is to resolve the conflicting aims of protecting IT systems against third-party attacks that exploit unknown IT security vulnerabilities on the one hand, and on the other hand keeping such vulnerabilities open so that source telecommunications surveillance can be carried out for public security purposes.

3. **Constitutional complaints asserting that the legislator has breached its duty of protection must satisfy a special burden of substantiation. Such constitutional complaints must address the entire legislative context, which requires that the relevant provisions of the legislative framework challenged by the constitutional complaint are at least outlined and that reasons are given as to why they provide insufficient protection under constitutional law.**

4. **Where a constitutional complaint directly challenges legislation, it may be necessary – in accordance with the principle of subsidiarity – for the complainants to file a declaratory action or an action for an injunction with the administrative courts before lodging their complaint. This is not necessary where the assessment of a law raises only specific questions of constitutional law, without any improved basis for decision-making to be expected from a prior examination carried out by the ordinary courts (established case-law). These principles also apply to constitutional complaints asserting that the legislator has breached its duty of protection.**

FEDERAL CONSTITUTIONAL COURT

- 1 BvR 2771/18 -

IN THE NAME OF THE PEOPLE

In the proceedings
on
the constitutional complaint

1. of Dr. K…,

2. of Mr M…,

3. of Mr W...,

4. of Mr F.-D...,

5. of the registered association C e.V...,
   represented by its board members,

6. of the registered cooperative I... eG,
   represented by its board members,

7. of the civil-law partnership O… GbR,
   represented by its managing directors,

- authorised representative: … -

against § 54(2) of the Baden-Württemberg Police Act (*Polizeigesetz Baden-Württemberg*) in the version of the Act to Implement Directive (EU) 2016/680 for the Police in Baden-Württemberg and to Amend Other Police Law Provisions (*Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 für die Polizei in Baden-Württemberg und zur Änderung weiterer polizeirechtlicher Vorschriften*) of 6 October 2020 (Baden-Württemberg Law Gazette, *Gesetzblatt*, page 735)

the Federal Constitutional Court - First Senate -

with the participation of Justices:

President Harbarth,

Paulus,

Baer,

Britz,

Ott,

Christ,

Radtke,

Härtel

held on 8 June 2021:

The constitutional complaint is dismissed as inadmissible.

R e a s o n s:

A.

[*Excerpt from Press Release No. 62/2021 of 21 July 2021*

§ 54 of the Baden-Württemberg Police Act in the version of 6 October 2020 (*Polizeigesetz Baden-Württemberg* – PolG BW) allows for the covert surveillance of the contents of telecommunications for the purpose of preventive police work in order to protect certain weighty legal interests. Pursuant to § 54(2) PolG BW, which is the provision challenged by the complainants in these proceedings, surveillance may be carried out through interference with IT systems if technical measures are in place to ensure that telecommunications are only intercepted and recorded in real time and if the interference is necessary to intercept and record telecommunications, particularly in unencrypted form. Performing this kind of source telecommunications surveillance under § 54(2) PolG BW involves infiltrating the targeted system with surveillance software. This can be done in various ways. The constitutional complaint solely concerns infiltration by way of exploiting zero-day vulnerabilities in the hardware or software of the targeted system.

The complainants essentially assert that, by enacting the authorisation laid down in § 54(2) PolG BW, the *Land* Baden-Württemberg violated the right to protection of the confidentiality and integrity of information technology systems – as guaranteed by fundamental rights – because the authorities have no interest in notifying developers of any vulnerabilities that come to their attention since they can exploit these vulnerabilities to infiltrate IT systems for the purpose of source telecommunications surveillance, which is permitted under § 54(2) PolG BW. Yet if the developers are not notified, these vulnerabilities and the associated risks – in particular the risk of third-party attacks on IT systems – will continue to exist. The complainants contend that it would have been absolutely necessary for Baden-Württemberg to create a legal framework providing for a vulnerability management system that would have to prohibit the exploitation of security vulnerabilities unknown to the developer of the respective system. They argue that even if the exploitation of zero-day vulnerabilities were not

deemed inherently incompatible with the state's duty of protection, administrative procedures must at least be established for evaluating IT security vulnerabilities on a case-by-case basis.

End of excerpt]

[…] 1

I.

[…] 2-7

II.

[…] 8-11

III.

[…] 12-19

B.

The constitutional complaint is inadmissible because the complainants have failed to sufficiently substantiate the alleged breach of the duty of protection and have not met the requirements arising from the principle of subsidiarity in a broader sense. 20

I.

In principle, the complainants can be holders of fundamental rights and thus have legal ability to lodge a complaint. This also applies to complainants nos. 5 to 7 that, as a registered association (cf. Decisions of the Federal Constitutional Court, *Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 3, 383 <390>; 10, 221 <225>; 24, 278 <282>; 97, 228 <253>; 105, 279 <292 f.>), a registered cooperative (cf. BVerfGE 118, 168 <168, 203>) and a civil-law partnership (*Gesellschaft des bürgerlichen Rechts*) (cf. Federal Constitutional Court, Order of the First Chamber of the First Senate of 2 September 2002 - 1 BvR 1103/02 -, para. 6), are holders of fundamental rights in their capacity as domestic legal persons within the meaning of Art. 19(3) of the Basic Law (*Grundgesetz* – GG). Legal persons can generally invoke the right to protection of the confidentiality and integrity of information technology systems asserted by the complainants, insofar as this right is not based on Art. 1(1) GG ([…]). In this context, their need for protection resembles that of natural persons. However, there is a difference in that the protected activities of legal persons, unlike those of natural persons, are typically limited by a specific purpose. The differences between the need for protection of natural and legal persons must be taken into consideration when determining the scope of this fundamental rights guarantee (cf. regarding the right to informational self-determination BVerfGE 118, 168 <203 f.>; 128, 1 <43>; cf. regarding Art. 10(1) GG BVerfGE 100, 313 <356>; 106, 28 <43>; 107, 299 <310>). 21

II.

The constitutional complaint has an admissible subject matter. The complainants directly challenge § 54(2) PolG BW. […] Their complaint is directed against a legal provision that they consider to be insufficient from a fundamental rights perspective. This is an admissible challenge (cf. most recently Federal Constitutional Court, Order of the First Senate of 24 March 2021 - 1 BvR 2656/18 inter alia -, para. 95 - Climate Change). 22

III.

The 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 offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (JHA Directive) contains EU data protection rules applicable to the present constellation, but this does not preclude the admissibility of the constitutional complaint. Neither the challenged provision as such nor the legislative elements that are lacking according to the complainants are fully determined by EU law (cf. BVerfGE 121, 1 <15>; 125, 260 <306 f.>; 130, 151 <177 f.>; 133, 277 <313 f. para. 88>; 152, 152 <168 para. 39>; 152, 216 <233 para. 42 f.>; 154, 152 <214 f. para. 84>; 155, 119 <165 para. 87>). 23

IV.

The complainants complied with the one-year time limit within which a constitutional complaint challenging legislation may be lodged pursuant to § 93(3) of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz* – BVerfGG). […] 24

V.

However, the complainants failed to satisfy the requirements of § 23(1) second sentence and § 92 BVerfGG, according to which they must demonstrate that they have standing to lodge the constitutional complaint. Pursuant to Art. 93(1) no. 4a GG and § 90(1) BVerfGG, a constitutional complaint can only be admissible if the complainants assert that one of their fundamental rights – or rights equivalent to fundamental rights – has been violated by public authority and if such a violation appears at least possible (cf. BVerfGE 79, 1 <13 ff.>; 83, 216 <226>; 83, 341 <351 f.>; 129, 49 <67>). The present constitutional complaint does not satisfy these requirements. In the present case, fundamental rights do give rise to a duty of protection (see 1. below), and the complainants have sufficiently demonstrated that their fundamental rights are individually, presently and directly affected (see 2. below). However, it is not sufficiently evident from the constitutional complaint that the duty of protection could have been violated (see 3. below). 25

1. Within the context of fundamental rights protection, the state bears a responsibil- 26

ity for the security of IT systems. In the circumstances under review in the present case, where the authorities are aware of a vulnerability that is unknown to the developer, the state has a specific duty of protection arising from fundamental rights. The state is obliged to help protect the users of IT systems against third-party attacks on those systems.

a) The privacy of telecommunications is affected in this case, as is the protection of the confidentiality and integrity of information technology systems, which is guaranteed by fundamental rights. 27

Insofar as third parties intercept the contents and circumstances of ongoing telecommunications when accessing a system, the privacy of telecommunications protected by Art. 10(1) GG is affected (cf. BVerfGE 120, 274 <307>; 141, 220 <309 para. 228>). 28

In all other cases, the infiltration of an IT system affects the right to protection of the confidentiality and integrity of information technology systems derived from Art. 2(1) in conjunction with Art. 1(1) GG (cf. BVerfGE 120, 274 <307 ff.>). It is true that the challenged provision only allows the competent authorities to carry out source telecommunications surveillance in respect of ongoing telecommunications (cf. § 54(2) no. 1 PolG BW), which means that state interferences on the basis of § 54(2) PolG BW would have to be measured against Art. 10(1) GG. However, if third parties infiltrate a system through an unknown security vulnerability, they could gain access not just to ongoing telecommunications, but also to the entire IT system and its data. They can then spy on the system, manipulate it, and blackmail users by threatening to manipulate, and especially to destroy, data. 29

b) Fundamental rights are affected here in their protective dimension, thereby imposing a specific duty of protection on the state. 30

aa) According to the Federal Constitutional Court’s established case-law, fundamental rights not only guarantee the individual a defensive right against state interference, but also constitute an objective decision on constitutional values that establishes duties of protection on the part of the state (cf. BVerfGE 39, 1 <42>; established case-law). 31

Art. 10(1) GG not only gives rise to a defensive right against state interference, but also requires the state to protect individuals from private third parties gaining access to communications that are protected by the privacy of telecommunications (cf. BVerfGE 106, 28 <37>, regarding the protection afforded by the fundamental right to informational self-determination cf. Federal Constitutional Court, Order of the Third Chamber of the First Senate of 17 July 2013 - 1 BvR 3167/08 -, para. 19 f.; regarding the permeating effect of fundamental rights on private law cf. BVerfGE 152, 152 <189 ff. para. 85 ff.> - Right to be forgotten I). 32

For its part, the right to protection of the confidentiality and integrity of information technology systems also has a protective dimension. From a fundamental rights per- 33

spective, the particular need for protection follows from the fact that users rely on IT systems for their freedom and the general development of their personality; it also follows from the risks to one's personality resulting from the use of such IT systems (cf. already BVerfGE 120, 274 <306>). The Court already set out in 2008 to what degree free development of the individual, which is protected by fundamental rights, now requires the use of information technology (loc. cit., p. 303 ff.). Since then, the connection between free development [of one's personality] and information technology has only become stronger. The change from analogue to digital processes and the increasingly widespread mobile use of IT systems are leading to ever greater dependence on information technology. It is becoming increasingly difficult for individuals to exercise their fundamental freedoms without using IT systems, and it is also becoming increasingly less feasible to avoid the risks associated with the use of IT systems by refraining from such use. In light of this, the fundamental rights do not just require that the state respect users' legitimate expectations regarding the integrity and confidentiality of such systems (cf. BVerfGE 120, 274 <306>). The state is also obliged to help protect the integrity and confidentiality of IT systems from third-party attacks ([…]).

bb) If the state is aware of security vulnerabilities unknown to developers and users, the general mandate of protection consolidates into a specific duty of protection that arises from fundamental rights, requiring the state to protect users of IT systems from third-party infiltration of the systems by way of unknown security vulnerabilities (see (1) below). This specific duty of protection incumbent upon the state does not preclude state authorities from carrying out source telecommunications surveillance using an unknown security vulnerability. However, it does require a legal framework that governs how the state is to resolve the conflicting aims of protecting IT systems against third-party infiltration on the one hand, and preserving the possibility of carrying out source telecommunications surveillance by exploiting unknown security vulnerabilities for public security purposes on the other (see (2) below). 34

(1) If state authorities become aware of security vulnerabilities, the state's general mandate of protection consolidates into a specific duty of protection (regarding Art. 2(2) first sentence GG cf. BVerfGE 142, 313 <338 para. 71>). This specific duty of protection arises given that security vulnerabilities can potentially cause major damage (see (a) below), affected persons are unable to protect themselves against this damage (see (b) below) and a state authority is aware of the security vulnerabilities (see (c) below). 35

(a) If security vulnerabilities are kept open, they entail special risks to informational self-determination. Information technology systems allow for a wide range of possible uses involving the creation, processing and storage of data. Anyone with access to this data can obtain extensive knowledge about users' personalities (in more detail BVerfGE 120, 274 <305 f.>). Where the technical infiltration of a complex information technology system is undertaken, this infiltration is the critical step that makes it possible to spy on the system as a whole and thus to obtain extensive information (cf. 36

BVerfGE 120, 274 <308 f.>).

Moreover, given the diverse uses of IT systems and the fact that users are generally reliant on such systems, security vulnerabilities have the potential to cause damage far greater than the disclosure of personal information – for example by disrupting industrial and commercial processes. Third parties that infiltrate and manipulate IT systems via security vulnerabilities are capable of disrupting a large variety of processes, causing damage to affected persons. The risk of being infiltrated by third parties is also associated with the particular risk of being blackmailed. 37

These risks are considerable because it must be assumed that there are many undetected vulnerabilities. The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) recommends assuming that any software used contains vulnerabilities (assume breach paradigm, cf. Federal Office for Information Security, The State of IT Security in Germany 2017, p. 18; The State of IT Security in Germany 2019, p. 8; The State of IT Security in Germany 2020, pp. 22 ff., 34, 44 f., 79, 81). 38

(b) In general, individuals cannot effectively protect themselves against the risk of third parties exploiting zero-day vulnerabilities that developers are not aware of and that therefore cannot be fixed by updating the system. They will not always be able to detect such third-party access; in any case, they have only limited powers to prevent it (cf. BVerfGE 120, 274 <305 f.>). 39

(c) In the circumstances under review here, it is the competent authorities themselves that are aware of such vulnerabilities, and that could therefore remedy this problem. The complainants do not claim that the authorities would have to actively search for security vulnerabilities. Rather, they demand that vulnerabilities that have come to the authorities' attention, but are unknown to the developers, be handled in ways that protect fundamental rights. Therefore, the constitutional complaint only concerns constellations where the authorities are aware of a security vulnerability, either because they discovered it themselves or obtained the knowledge from third parties. The special obligation of the state to protect users follows specifically from the fact that the state has this knowledge, while the developers are unaware of it and affected persons have no way of protecting themselves (cf. also BVerfGE 142, 313 <338 f. para. 73> regarding Art. 2(2) first sentence GG). 40

(2) The duty of protection makes it incumbent upon the legislator to set out how the police authorities are to handle security vulnerabilities of which developers are not aware. 41

If there were no authorisation to carry out source telecommunications surveillance, and it were not therefore in the authorities' interest to exploit security vulnerabilities to infiltrate IT systems, the authorities would regularly notify developers of vulnerabilities brought to their attention so that the developers could fix them. However, when an authority is permitted to carry out source telecommunications surveillance for pub- 42

lic security purposes, this creates a conflict between the public interest in having the highest possible level of IT security on the one hand and the possibility of carrying out source surveillance to protect other high-ranking legal interests on the other. As a consequence, there is a risk that the authority will refrain from suggesting that the vulnerability be closed, or even actively work towards ensuring that the vulnerability remains undetected (cf. already BVerfGE 120, 274 <326> regarding remote searches). Moreover, the mere fact that certain state authorities are permitted to carry out surveillance could create an incentive for third parties not to notify the developers of security vulnerabilities they have discovered and instead to offer this information to state authorities in return for payment. This increases the risk that security vulnerabilities are not reported to the developers.

Due to these risks to the security of IT systems, source telecommunications surveillance performed by exploiting unknown security vulnerabilities is subject to stricter justification requirements, but it is not inherently impermissible under constitutional law (regarding remote searches cf. BVerfGE 120, 274 <325 f., 328>; 141, 220 <304 f. para. 211 f.>). The protection of the confidentiality and integrity of information technology systems therefore does not grant individuals a right to have source telecommunications surveillance exploiting unknown security vulnerabilities banned altogether. Nor does it give rise to a claim that authorities must notify developers about any IT security vulnerabilities immediately and in all circumstances. 43

However, the duty of protection arising from fundamental rights does require a legal framework that governs how the authority, when deciding on keeping unknown security vulnerabilities open, is to resolve the conflicting aims of protecting IT systems against third-party infiltration on the one hand, and preserving the possibility of carrying out source telecommunications surveillance on the other. If an authority becomes aware of a zero-day vulnerability, said authority must be required to balance these conflicting interests. It must be ensured that every time the authority decides whether to keep an unknown security vulnerability open, it assesses the risk of the vulnerability's existence becoming more widely known and it determines, in qualitative and quantitative terms, the benefit of potential state infiltration measures exploiting the vulnerability. Following a weighing of the risks and benefits, the authority must report the security vulnerability to the developer unless the interest in keeping it open outweighs the risks. 44

2. The complainants have shown that a violation of the duty of protection would individually, directly and presently affect them. 45

They have demonstrated that they are individually affected given that they use IT systems that potentially have unknown vulnerabilities and that could thus be infiltrated by third parties. While many citizens presumably face this risk, it is not required that the complainants demonstrate how they are individually affected in more detail. In constitutional complaint proceedings, it is not generally required that complainants are especially affected – beyond simply being individually affected – in some particu- 46

lar manner that differentiates them from all other persons (cf. Federal Constitutional Court, Order of the First Senate of 24 March 2021 - 1 BvR 2656/18 -, para. 110 – Climate Change).

The complainants are also directly and presently affected. The challenged provision entails the direct risk of (criminal) exploitation of unreported security vulnerabilities; this risk exists even if the authority has not made use of the authorisation to carry out source telecommunications surveillance. The complainants challenge the fact that § 54(2) PolG BW directly increases the risk that vulnerabilities that would be reported to and fixed by developers if there was no authorisation to carry out surveillance are not reported to them and can therefore also be exploited by third parties. This fact is not changed by the *Land* government's assertion that the authorities currently do not search for or collect vulnerabilities in the context of source telecommunications surveillance for the purpose of preventive police work. It cannot be inferred from this assertion that the competent authorities have not already obtained knowledge, incidentally or through other (public) bodies, of vulnerabilities, of which developers are not notified in light of § 54(2) PolG BW. 47

3. However, the complainants have not sufficiently demonstrated that the duty of protection arising from fundamental rights might have been violated. 48

a) There is an essential difference between the defensive rights of the individual against state interference that arise from fundamental rights on the one hand, and the state's duties of protection that result from the objective dimension of fundamental rights on the other. In terms of purpose and content, defensive rights are aimed at prohibiting certain forms of state conduct, whereas duties of protection are essentially unspecified. It is for the legislator to establish and implement a concept of protection. In this respect, the legislator generally has a margin of appreciation, assessment and manoeuvre, even if it is in principle obliged to take measures to protect a legal interest. This margin also gives the legislator latitude in taking into account conflicting public and private interests (cf. BVerfGE 96, 56 <64>; 121, 317 <356, 360>; 133, 59 <76 para. 45>; 142, 313 <337 para. 70>; established case-law). 49

The Federal Constitutional Court will only find a violation of such a duty of protection if no precautionary measures whatsoever have been taken, or if the adopted provisions and measures prove to be manifestly unsuitable or completely inadequate for achieving the required protection goal, or if the provisions and measures fall significantly short of the protection goal (regarding Art. 2(2) first sentence GG cf. most recently Federal Constitutional Court, Order of the First Senate of 24 March 2021 - 1 BvR 2656/18 inter alia -, para. 152 with further references - Climate Change; established case-law). Thus, the legislative decision on what measures to take to provide protection can only be reviewed by the Federal Constitutional Court to a limited extent. It is only in special circumstances that legislative latitude must be narrowed down to the taking of one specific measure as the only measure capable of giving effect to the state's duty of protection (cf. BVerfGE 56, 54 <73 ff.>; 77, 170 <214 f.>; 50

79, 174 <202>; 142, 313 <337 f. para. 70 f.>).

Constitutional complaints seeking a declaration that the legislator has violated its duty of protection must satisfy a special burden of substantiation. A possible violation of fundamental rights can generally only be derived from the complainants' submissions if the submissions go beyond general assertions and the selective highlighting of alleged inadequacies of the law. Complainants must address the entire legislative context, which requires – depending on the specific case – that the relevant provisions of the legislative framework challenged by the complainants are at least outlined and that reasons are given as to why the legislative design is considered to fall short. 51

The Court's decision on the Climate Change Act does not merit a different conclusion. It is true that in that decision, the Court found that the complainants did not have to pinpoint all the relevant measures in order to establish their standing. But the reason that such precision could be dispensed with in that case is because the legislator itself had enacted a broad and general legal framework and the complainants could therefore limit themselves to challenging that framework (cf. Federal Constitutional Court, Order of the First Senate of 24 March 2021 - 1 BvR 2656/18 inter alia -, para. 134). This is not the case here. 52

b) The present constitutional complaint does not satisfy the substantiation requirements set out above. There are various legal provisions protecting IT systems, which – although their relevance under constitutional law cannot be definitively determined here – might be significant in the present context. In their constitutional complaint, the complainants did not outline the existing provisions, nor did they state the specific reasons why it must be assumed that these provisions fail to provide protection. Insofar as they have made additional submissions in that regard in their brief of 10 March 2021, this is ultimately not sufficient to demonstrate a possible violation of the duty of protection. 53

aa) The statutory authorisation itself contains various safeguards that the legislator actually included with the specific aim of "protecting data security also with regard to third-party interferences" (*Landtag* document, *Landtagsdrucksache* – LTDrucks 16/2741, p. 31). The complainants would at least have needed to address § 54(3) second sentence PolG BW, which states that the method employed must be protected from unauthorised use. It is not ruled out from the outset that this provision leaves a margin of interpretation for adequately dealing with the conflict between the public interest in being able to infiltrate IT systems on the one hand, and in having the highest possible level of IT security on the other. 54

It is possible that the "methods" mentioned in § 54(3) second sentence PolG BW refer to the infiltration software, rather than the security vulnerabilities exploited to use this software, given that the vulnerability in the target system exists regardless of police action. However, when § 54(3) second sentence PolG BW is interpreted in ordinary law terms, the element of the "method employed" might have to include the 55

vulnerability to be exploited. This vulnerability would then have to be protected from unauthorised use – for example by notifying the developer. The complainants very briefly addressed this point in their additional submission of 10 March 2021. However, the time limit for lodging the constitutional complaint had already expired by that point, and this submission therefore does not comply with the time limit for lodging and providing reasons for a constitutional complaint (cf. BVerfGE 145, 20 <52 para. 79>). Nor was this submission a mere addition to a constitutional complaint that had already been sufficiently substantiated and was thus admissible (cf. in this respect BVerfGE 127, 87 <110>).

bb) The conflicting aims of the public interest in having state access to telecommunications and the highest possible level of IT security could also require examination in the context of a data protection impact assessment. This type of assessment is set out in § 80 PolG BW, which was inserted by amendment of 6 October 2020 to implement Art. 27 of the JHA Directive. […] 56

The complainants failed to address this point. Simply disregarding it on the grounds that the provision governing data protection impact assessments was only enacted after they lodged their constitutional complaint and after the time limit expired was not an option. Complainants must make additions to their submissions if the facts and the law change after expiry of the time limit (cf. BVerfGE 106, 210 <214 f.>). This applies in particular if they assert a violation of a duty of protection and a law enters into force, after expiry of the time limit, that might give effect to this duty of protection. Moreover, according to Art. 27 of the JHA Directive, the legislator had already been required to enact rules governing data protection impact assessments when the constitutional complaint was lodged, which means that the complainants should at least have addressed this EU rule before it was implemented in *Land* law. 57

It is uncertain whether such an impact assessment must be carried out in cases where a zero-day security vulnerability is kept open. But there is no doubt that a data protection impact assessment must be carried out prior to the use of surveillance software on the basis of § 54(2) PolG BW. It is less clear that this should also apply to the decision not to report to the developer a security vulnerability known to an authority, thus keeping it open. Yet Art. 27 of the JHA Directive, which § 80 PolG BW serves to implement, could indicate that such an assessment must also be carried out in those cases. The provisions reads as follows: 58

> Art. 27 JHA Directive
>
> Data protection impact assessment
>
> (1) Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the

impact of the envisaged processing operations on the protection of personal data.

(2) The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Art. 27 of the JHA Directive could warrant an interpretation of § 80 PolG BW according to which the provision not only addresses risks to the legal interests of persons who are directly or indirectly affected by the specific processing operation (in this case source telecommunications surveillance), but in principle also addresses risks to (other) persons. This is supported by the fact that Art. 27(1) of the JHA Directive refers to risks to the rights and freedoms of natural persons in general, and the fact that, even though Art. 27(2) of the JHA Directive distinguishes between data subjects and other persons concerned, the rights and legitimate interests of both groups must be taken into account in the impact assessment. 59

But it is also uncertain whether keeping open a security vulnerability is a “processing operation” within the meaning of § 80(1) PolG BW (regarding the element of “processing” see § 12 no. 2 PolG BW). It can at least not be ruled out that the processing operation must be considered a uniform matter that does not start with the interception of data taking place when the actual surveillance of telecommunications occurs, but also covers prior steps taken in preparation of such surveillance. Thus, keeping open a security vulnerability known to an authority could be considered a preparatory step before source telecommunications surveillance is carried out and would then be covered by § 80 PolG BW. The question whether the risk at issue here, which is that third parties exploit the vulnerability to infiltrate the IT system, is considered an “impact” of the processing operation (the operation being the keeping open of the security vulnerability) would require further clarification. 60

The complainants did not address these questions. It is not the Federal Constitutional Court’s task to conduct its own analysis of ordinary law, interpreting provisions that might provide protection as to whether they give effect to the constitutional duty of protection or fall short. 61

In the present constitutional complaint proceedings, the Federal Constitutional Court is also unable to request a preliminary ruling pursuant to Art. 267 TFEU regarding the interpretation of the EU provision governing impact assessments (Art. 27 JHA Directive). This is because the constitutional complaint is inadmissible and this question is therefore not relevant to the decision. Moreover, even if Art. 27 of the JHA Directive did not require an impact assessment for zero-day security vulnerabilities, it 62

would be unlikely to stand in the way of a broader interpretation of § 80 PolG BW (cf. Art. 1(3) JHA Directive). Even if the constitutional complaint were admissible, the interpretation of Art. 27 of the JHA Directive would therefore not be relevant to the decision of the Federal Constitutional Court.

cc) Nor do the complainants sufficiently address the extent to which Baden-Württemberg legislation on cybersecurity contains safeguards. The Act to Improve Cybersecurity and Amend Other Provisions (GBl 2021, p. 182, hereinafter: Cybersecurity Act, *Cybersicherheitsgesetz* – CSG) entered into force on 17 February 2021. The Act provides for the Baden-Württemberg Cybersecurity Agency (cf. § 1(1), § 3 CSG). This agency is to serve as a central coordination and reporting unit for the cooperation of public bodies in matters of cybersecurity in Baden-Württemberg (cf. § 4(1) CSG) and, in particular, to collect and evaluate all information necessary for averting threats to cybersecurity, including information on security vulnerabilities (cf. § 4(2) no. 1 CSG). From January 2022, the Cybersecurity Act will also give rise to obligations on the part of *Land* authorities to report security vulnerabilities to the Cybersecurity Agency (cf. § 4(3) CSG), and confer upon the agency powers to avert threats to cybersecurity (cf. § 5 CSG). The Cybersecurity Agency will also be authorised to issue warnings, recommendations and notices regarding security vulnerabilities to the public or affected groups – usually after prior consultation with the developer (cf. § 8(1) CSG). 63

The fact that the Cybersecurity Act only entered into force after the constitutional complaint had been lodged and the time limit had expired (see para. 57 above) does not excuse the complainants from having to make submissions in this regard in the constitutional complaint proceedings. It is true that the complainants' additional submissions of 10 March 2021 regarding the Cybersecurity Act do have to be taken into consideration because the Act only entered into force on 17 February 2021, precluding the complainants from making such submissions within the time limit. However, these additional submissions do not satisfy the substantiation requirements either. The entire system of safeguards must be addressed in order to substantiate a potential violation of a duty of protection; it is not sufficient to merely selectively highlight an individual provision that may be inadequate. Above all, the complainants did not address the question whether the relevant provisions could be interpreted to the effect that they afford fundamental rights protection that is sufficient under constitutional law against third-party attacks on IT systems. 64

dd) Finally, the complainants do not address the reporting standard, which is governed by delegated legislation. On 5 October 2017, the IT Planning Council adopted a "binding procedure for reporting IT security incidents to allow for information sharing within the Administrative Network of Computer Emergency Response Teams (reporting standard)" (No. 2017/35) within the scope of the Treaty on the Establishment of the IT Planning Council and on the Principles of Cooperation Underlying the Use of Information Technology in the Administrations of the Federation and the *Länder* – Treaty to Implement Article 91c GG (IT State Treaty in the version published on 13 65

December 2019, Federal Law Gazette, *Bundesgesetzblatt* – BGBl I p. 2852). This resulted in a binding agreement (cf. § 2(2) second sentence IT State Treaty) on an IT security standard within the meaning of § 3(1) (now § 2(1)) of the IT State Treaty in respect of information sharing between the Federation and the *Länder*, requiring that IT security incidents that might have an impact on the *Länder* or the Federation or that are considered to be relevant for others must be reported (§ 2(1) of the decision). Such incidents must be reported to the Federal Office for Information Security, among other bodies. The reporting obligation also extends to novel security vulnerabilities in IT products (cf. § 2(2) in conjunction with Annex 1 of the decision). Pursuant to § 3 of the decision, such incidents must be reported by the Federation and the *Länder*. Thus, it is at least conceivable that the Federal Office for Information Security could, and should, take into account the duties of protection arising from fundamental rights when using its discretion with regard to decisions on how to deal with such knowledge – in particular decisions to issue warnings about security vulnerabilities in IT systems to the public or affected groups pursuant to § 7(1) first sentence no. 1(a) of the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* – BSIG) and to notify developers.

The extent to which effect can be given to the constitutional duty of protection through reporting obligations set out in delegated legislation – and whether this delegated legislation is itself based on sound legislative foundations – would require further examination. The complainants should have discussed this aspect in their submissions as well, given that the reporting standard could be an element of a legislative framework protecting against the impermissible exploitation of vulnerabilities by third parties. 66

VI.

Furthermore, the constitutional complaint is inadmissible because it fails to satisfy the requirements arising from the principle of subsidiarity in a broader sense. 67

1. a) Exhausting the remedies formally available for achieving the immediate aim of legal action is not sufficient for fulfilling the subsidiarity requirements; rather, all options that might remedy the alleged fundamental rights violation must be pursued. This serves the purpose of ensuring that the Federal Constitutional Court does not have to take far-reaching decisions on an uncertain factual and legal basis. It is the ordinary courts – which are primarily responsible for the interpretation and application of ordinary law – that must first address the points of fact and law at issue. 68

The principle of subsidiarity therefore generally requires that, before lodging a constitutional complaint, the complainants first pursue all available procedural options that might remedy the alleged violation of the Constitution or prevent a fundamental rights violation. This also applies if it is unclear whether the type of remedy sought is in principle admissible and all other admissibility requirements are met in the specific case. 69

If a constitutional complaint directly challenges legislation, the legal remedies that need to have been sought beforehand may include the filing of a declaratory action or an action for an injunction with the administrative courts. This applies even if the provisions at issue are exhaustive [i.e. leave no room for interpretation] and the best possible outcome of a review by the ordinary courts is that the challenged law is referred to the Federal Constitutional Court pursuant to Art. 100(1) GG. In this respect, too, it is decisive whether prior review by the ordinary courts is necessary to avoid a situation in which the Federal Constitutional Court has to decide on an uncertain factual and legal basis. This will typically be the case if the challenged provisions contain legal terms that are subject to interpretation, and where the interpretation and application of these terms significantly influence the extent to which complainants are adversely affected, both with regard to the facts and the law (cf. BVerfGE 143, 246 <321 f. para. 210>; 145, 20 <54 f. para. 85 f.>; 150, 309 <326 f. para. 42 ff.>). 70

By contrast, where the assessment of a provision raises only specific questions of constitutional law that are for the Federal Constitutional Court to answer, without any improved basis for decision-making to be expected from a prior examination carried out by the ordinary courts, there is no need for such prior decision (cf. BVerfGE 150, 309 <326 f. para. 44> with further references). Moreover, complainants are not required to satisfy the principle of subsidiarity by breaking a law and exposing themselves to the risk of criminal punishment or an administrative fine so as to then be able to challenge the provision as unconstitutional in criminal proceedings or administrative fining proceedings (cf. BVerfGE 145, 20 <54 para. 85> with further references). Exceptions from the obligation to have recourse to the ordinary courts before lodging a constitutional complaint also apply if the challenged provisions compel the complainants to make substantial arrangements that cannot be reversed later, or if recourse to the ordinary courts is clearly pointless or futile, or if it is unreasonable (*nicht zumutbar*) for other reasons (cf. BVerfGE 150, 309 <327 f. para. 45> with further references). However, recourse to the ordinary courts may not be considered to be inherently futile simply on the grounds that the courts have not yet held that the legal remedy is admissible for the constellation in question (cf. BVerfGE 145, 20 <54 para. 85>). 71

b) These principles also apply to challenges asserting that the legislator has breached its duty of protection. In many cases, the existence of a gap in legal provisions relating to a specific matter can only be found with certainty if the ordinary courts have comprehensively addressed the facts of the case and the relevant ordinary law while taking into account constitutional standards. This avoids a situation in which the Federal Constitutional Court has to decide on an uncertain factual and ordinary law basis, including in cases where the legislator has failed to act. 72

2. The present constitutional complaint does not satisfy these standards. In the case at hand, complex questions arise concerning the interpretation of ordinary law. Whether, under the law as it currently stands, authorities are already required to carry out a balancing that gives effect to the duty of protection arising from fundamental 73

rights before deciding not to notify the developer of a zero-day vulnerability that has come to their attention depends on how various provisions of police law, data protection law, cybersecurity law and IT security law are interpreted (see para. 53 ff. above). These areas of law are largely part of more recent ordinary law and their significance has not yet been precisely delineated through court decisions, other applications of the law or legal scholarship. To ensure that the Federal Constitutional Court does not have to make decisions on an uncertain factual and legal basis, the ordinary courts – which are primarily responsible for the interpretation and application of ordinary law – must first be given the opportunity to assess the points of fact and law at issue. Therefore, the complainants would have had to try to obtain legal protection from the ordinary courts by filing a declaratory action or a preventive action for an injunction with the administrative courts. In light of the more recent case-law of the administrative courts, it does appear possible that legal protection from the ordinary courts could be obtained with regard to the question of whether the fundamental rights of IT system users require (further) rules to ensure sufficient consideration of the protection of such IT systems from third-party infiltration when state authorities decide whether to keep open unknown security vulnerabilities for potential use of source telecommunications surveillance (regarding the admissibility of a negative declaratory action cf. Decisions of the Federal Administrative Court, *Entscheidungen des Bundesverwaltungsgerichts* – BVerwGE 157, 8 <10 f. para. 13 >; 157, 126 <128 f. para. 15>; regarding a preventive action for an injunction cf. Federal Administrative Court, Judgment of 22 October 2014 - 6 C 7/13 -, para. 15 ff.; Judgment of 13 December 2017 - 6 A 6/16 -, para. 14; BVerwGE 161, 76 <77 f. para. 12 ff.>).

There are no evident reasons why the complainants cannot reasonably be expected to exhaust all legal remedies before the ordinary courts. In particular, the Federal Constitutional Court had already addressed the requirement of filing a declaratory action or an action for an injunction with the administrative courts on several occasions before the complainants lodged their constitutional complaint (cf. BVerfGE 143, 246 <321 f. para. 210>; 145, 20 <54 f. para. 86>; after expiry of the time limit for lodging a complaint, but before the insertion of § 80 PolG BW and the adoption of the Baden-Württemberg Cybersecurity Act cf. also BVerfGE 150, 309 <326 f. para. 42 ff.> - Automatic number plate recognition in Baden-Württemberg and Hesse). 74

Harbarth Paulus Baer

Britz Ott Christ

Radtke Härtel

Bundesverfassungsgericht, Beschluss des Ersten Senats vom 8. Juni 2021 - 1 BvR 2771/18

Zitiervorschlag BVerfG, Beschluss des Ersten Senats vom 8. Juni 2021 - 1 BvR 2771/18 - Rn. (1 - 74), http://www.bverfg.de/e/rs20210608_1bvr277118en.html

ECLI ECLI:DE:BVerfG:2021:rs20210608.1bvr277118