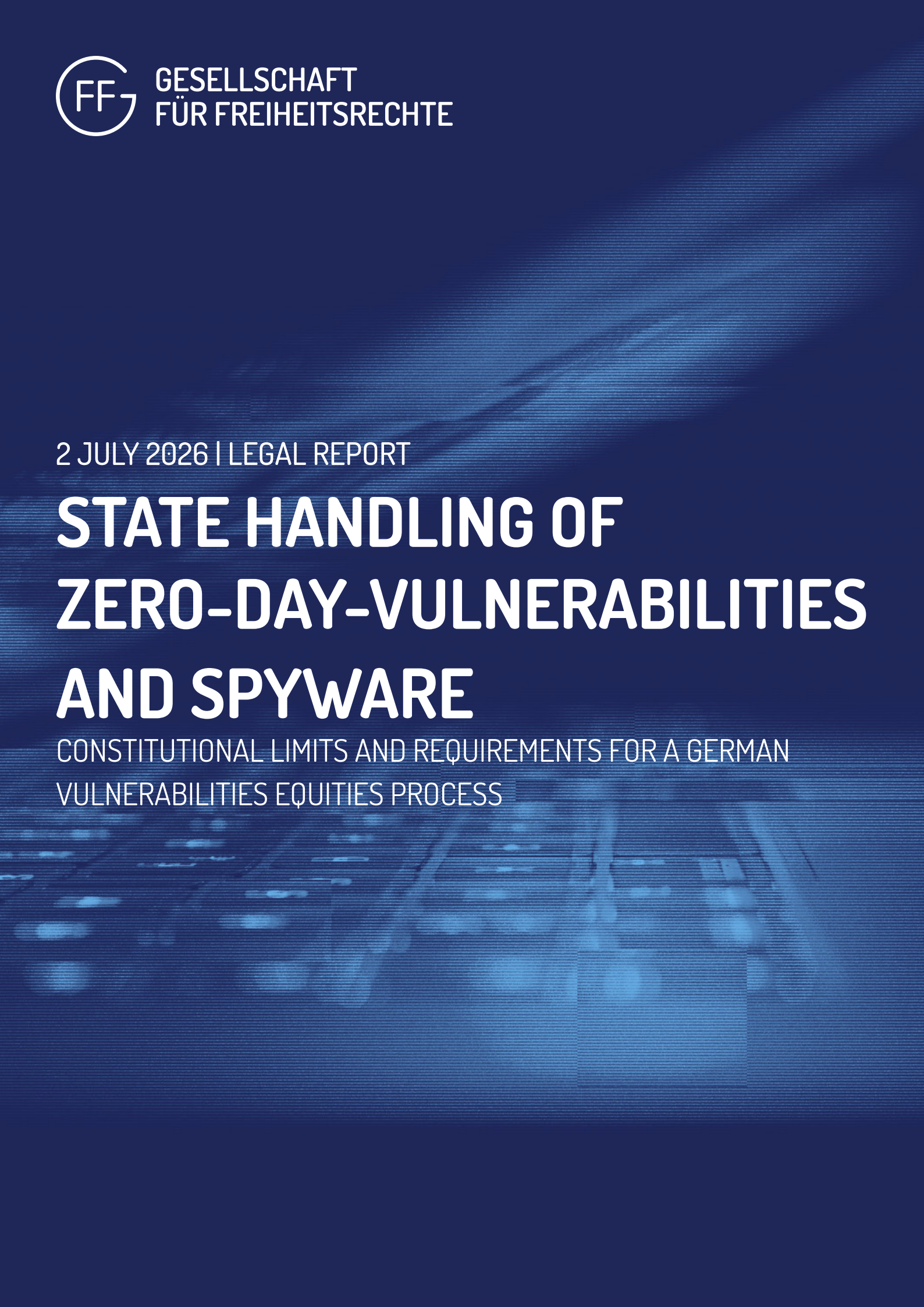
GESELLSCHAFT
FÜR FREIHEITSRECHTE

2 JULY 2026 | LEGAL REPORT

STATE HANDLING OF ZERO-DAY-VULNERABILITIES AND SPYWARE

CONSTITUTIONAL LIMITS AND REQUIREMENTS FOR A GERMAN VULNERABILITIES EQUITIES PROCESS



GESELLSCHAFT
FÜR FREIHEITSRECHTE

IMPRINT

Gesellschaft für Freiheitsrechte e.V.

Boyenstr. 41

10115 Berlin

Phone +49 30 549 08 10 – 0

Fax +49 30 549 08 10 – 99

info@freiheitsrechte.org

PGP/GPG Key ID FA2C23A8

Bank details

IBAN: DE 88 4306 0967 1182 9121 00

BIC: GENODEM1GLS

GLS Gemeinschaftsbank eG

Represented by the association's board

Prof. Dr. Nora Markard

Prof. Dr. Boris Burghardt

Dr. John Philipp Thurn

Prof. Dr. Dana-Sophia Valentiner

Felix Reda

Prof. Dr. Leonie Steinl LL.M.

Editorially responsible

Malte Spitz

Boyenstr. 41

10115 Berlin

Authors

Prof. Dr. Thomas Wischmeyer

Dr. Paul Friedl

Cover image

unsplash.com | Philipp Katzenberger

Layout

Bernhard Leitner

Translation note

This document is a machine-generated English translation of a legal report (*Rechtsgutachten*) originally written and published in German, available at https://freiheitsrechte.org/uploads/publications/Digital/Rechtsgutachten-Spyware.pdf. The translation is provided to make the report's findings accessible to an English-speaking audience.

The German original is the authoritative version. It was published on 2 July, 2026, and this translation reflects that version. Anyone wishing to quote or rely on the report's findings should refer to and cite the German original rather than this translation.

The translation has been reviewed for overall comprehensibility. It has not been professionally edited, revised, or proofread, and it may contain errors. German legal terminology without a settled English equivalent — including statute names, institutional names, and doctrinal terms — has been rendered as closely as possible and in places retained in German.

Where official or published English-language versions of cited materials exist — in particular for judgments of the Bundesverfassungsgericht and the Court of Justice of the European Union, and for EU legal acts — the report uses those versions; readers relying on them should verify against the authoritative version. Sources originally written in English are quoted in their original wording. Other quotations have been translated from German into English.

Table of contents

Executive Summary

So-called *zero-day vulnerabilities* – IT security flaws unknown to the vendors whose products they affect – pose serious risks to both civil liberties and public security. They create attack vectors that hostile actors can use to spy on German politicians and businesses, to surveil journalists and dissidents at home and abroad, and to sabotage critical infrastructure. Basic information security principles therefore require that such vulnerabilities, once discovered, be reported promptly to the affected vendors for patching.

State authorities, however, do not always choose to disclose what they find. They have their own reasons to keep vulnerabilities secret: law enforcement and intelligence agencies exploit zero-day vulnerabilities to intercept the communications of suspects and other surveillance targets, while military and security agencies deploy them in offensive cyber operations. When the state learns of a zero-day vulnerability, it thus faces a dilemma: disclosure protects the public, government, and economy, but the vulnerability may also be operationally valuable to security agencies carrying out their statutory functions.

Germany's Constitution, the *Grundgesetz*, requires the legislature to resolve this dilemma through a formal act of parliament that establishes binding rules for both the state's handling of unknown IT vulnerabilities and its use of third-party spyware. This obligation follows directly from the Federal Constitutional Court's 2021 decision on IT Security Vulnerabilities („*IT-Schwachstellen*“) and the broader body of relevant constitutional case law. Germany currently has no such legislation. That gap means the legislature is in breach of its constitutional duty; most importantly, its duty to protect the fundamental right to the integrity and confidentiality of IT systems. “”

The content that legislation must cover falls into two categories: constitutionally mandatory requirements and politically advisable recommendations that go beyond them.

On the mandatory side, any decision to retain an unknown vulnerability rather than disclose it must be made through a structured procedure that weighs the operational value of keeping it secret against the security risks of doing so. The legislation must establish a presumption in favour of disclosure: vulnerabilities may be withheld only temporarily and only in exceptional circumstances. It must designate a responsible decision-making body and set out the core elements of the procedure. Where a vulnerability is withheld, the legislation must require that steps be taken to mitigate the resulting information security risks and that the decision be revisited periodically. Withheld vulnerabilities must be protected against loss or theft through robust information security measures. The framework must also provide for independent oversight with the information, expertise, and resources needed to scrutinise decisions effectively.

Beyond these requirements, the legislature has room to make its own choices about the details of the process. With respect to the institutional hosting of the decision-making process and the specific procedure to be followed, it appears sensible not to leave this to a single authority, but rather to assign it to a cross-agency and interministerial body that decides on a consensual basis as a matter of principle and that has an adequately resourced secretariat at its disposal. On oversight and review, constitutional considerations favor a comprehensive review of legality, allowing every decision to withhold a vulnerability to be scrutinized independently. The remaining regulatory details can and should be left to secondary legislation..

The legislature must also regulate the state's use of surveillance capabilities supplied by third parties – commercial spyware vendors and allied foreign intelligence services. For these activities, too, are highly sensitive from a fundamental-rights perspective. Moreover, without such regulation, the constitutional duty to manage vulnerabilities would risk being rendered ineffective or circumvented. In doing so, the legislature must ensure that state authorities do not draw on surveillance capabilities that create unacceptable risks to constitutionally protected freedoms and securities. For commercially procured spyware, that means not only a vendor and product

assessment process comparable to the vulnerability management framework, but also accompanying safeguards – such as contractual data security requirements imposed on suppliers. A whitelist model or an outright ban on commercial spyware would equally be worth considering.

The federal legislature has the authority to enact these legislative projects. The EU holds no exclusive competence in this area, and existing EU law does not substantially constrain national action. Within Germany, however, the federation's direct legislative authority extends only to its own federal agencies; separate cooperative arrangements would be needed to cover how *Länder* authorities handle vulnerabilities and spyware.

Legal Opinion

A. Introduction

In today's digital society, ensuring an adequate level of information security is a basic precondition for the safe and reliable exercise of freedom. Information security ensures that private individuals — but also journalists and other professionals bound by duties of confidentiality — can communicate confidentially and without fear of surveillance. It also ensures that operators of critical infrastructure, from hospitals to electricity-grid operators, can reliably perform their supply functions, and that businesses can operate securely and are protected against cyberattacks. Accordingly, it is today largely undisputed that ensuring an adequate level of information security is a state task of fundamental importance.

Against this background, it may seem contradictory that the state itself creates and maintains considerable information insecurity. Yet this is precisely what happens when state bodies — security authorities in particular — do not report unknown IT vulnerabilities (so-called *zero-days*) to the affected vendors so that they can be remedied, but instead keep them secret in order to use them for their own operations (for example, surveillance measures).

The desire of state actors to hold such secret knowledge of vulnerabilities can be understandable: in an environment of largely encrypted communications infrastructure, the attack vectors created by vulnerabilities can be one of the few means of identifying and monitoring criminal actors.

The risks to freedom and security triggered by keeping vulnerabilities open are nonetheless enormous. Where the state keeps a vulnerability open, it generally cannot ensure that the vulnerability is not, at the same time or at some later point, exploited for illegitimate, illegal, or criminal purposes.

These are, after all, often the very same vulnerabilities that cybercriminals use to extort companies by means of *ransomware*, that foreign state actors use to carry out attacks on critical infrastructure, or that authoritarian regimes use to surveil dissidents.

The state thus finds itself in a dilemma: on the one hand, it must ensure effective threat prevention and criminal prosecution; on the other, it must also protect IT security and the freedoms bound up with it. The expansion of the offensive cyber capabilities of the BKA and the Bundespolizei (also known as "*hack backs*"), as proposed in the "Gesetz zur Stärkung der Cybersicherheit", which is expected to be passed by the Bundestag in 2026,[1] would further aggravate this existing conflict.

One means of resolving this dilemma in a structured way lies in implementing so-called *vulnerabilities equities processes* (VEPs). VEPs are a formal procedure — often laid down by statute — in which state authorities decide, by weighing the competing interests, whether a specific vulnerability is to be kept secret or reported to the affected vendor. Such processes have been publicly established, for example, in the United States,[2] the United Kingdom,[3]

---

[1] Federal Government of Germany, *Entwurf eines Gesetzes zur Stärkung der Cybersicherheit* (21.05.2026), § 41a BPolG-E und § 68d BKAG-E, abrufbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/cyberabwehr-RefE.pdf?__blob=publicationFile&v=4.

[2] *Vulnerabilities Equities Policy and Process for the United States Government* (*U.S. VEP*) (15.11.2017), https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/external%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[3] Government Communications Headquarters (GCHQ), *The Equities Process* (2018) abrufbar unter https://www.gchq.gov.uk/information/equities-process.

and Australia.[45] Comparable processes are also said to have been set up within certain authorities in other countries, though without more detailed information about these procedures being publicly known.[6]

In Germany, too, security authorities state that they operate internal vulnerability management.[7] As of yet, however, there are no statutory requirements governing how such procedures must be designed. This appears problematic not only in view of the existing opacity of these procedures and the high fundamental-rights relevance of the question set out at the outset: in its „*IT-Sicherheitslücken*“ decision of June 2021, the Bundesverfassungsgericht held that Germany’s Constitution, the *Grundgesetz*, requires a „framework for resolving, in a manner consistent with fundamental rights, the conflict between, on the one hand, protecting information technology systems against attacks by third parties through the disclosure of previously unknown security vulnerabilities and, on the other hand, retaining such vulnerabilities in order to enable source telecommunications surveillance for the purpose of threat prevention.“.[8] The Court did not, however, decide whether the fundamental rights-backed positive obligations underlying this legislative mandate were in fact being breached, holding that the constitutional complaint was not sufficiently

---

[4] Australian Signals Directorate, *Responsible Release Principles for Cyber Security Vulnerabilities* (2019) https://www.asd.gov.au/sites/default/files/2022-03/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf.

[5] The U.S. *Vulnerabilities Equities Process* (VEP) continues to shape the discourse, as it is widely regarded as the first publicly documented vulnerability management process worldwide.

[6] Herpig & Schwartz, *The Future of Vulnerabilities Equities Processes Around the World* (4. Januar 2019) https://www.lawfaremedia.org/article/future-vulnerabilities-equities-processes-around-world.

[7] Bundesministerium des Innern, für Bau und Heimat, *Cybersicherheitsstrategie für Deutschland 2021*, p 103 f.

[8] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Ls. 2.b) (*IT-Sicherheitslücken*).

substantiated on that point.[9] The legislature, accordingly, has likewise not yet taken action.

It thus remains unclear whether the state is constitutionally obliged to enact statutory rules on vulnerability management, whether — and if so, which — requirements for such vulnerability management follow from the „*IT-Sicherheitslücken*“ decision and the further case law of the Bundesverfassungsgericht, and what regulatory latitude may exist.

These questions are to be answered by the following report, which is divided into three parts. First, it examines which constitutional rules establish requirements and specifications for statutory rules on vulnerabilities (Part B.). To that end, the report discusses the extent to which the covert stockpiling of state knowledge of vulnerabilities restricts fundamental rights, which configurations of a vulnerability-management process are therefore constitutionally mandatory, and which options present themselves within the remaining regulatory latitude. The question of drawing on external knowledge of vulnerabilities — both from commercial spyware vendors and from allied third states — is addressed separately. The second part of the report then examines who, within the three-tiered competence structure between the European Union, the Federation, and the Länder, has the competence to enact statutory rules on vulnerability management (Part C.). It is shown that Germany is competent to regulate the handling of IT vulnerabilities and spyware and that existing EU law does not substantially restrict national legislatures in their regulatory authorities. Finally, on the basis of the constitutional analysis, a concrete proposal is formulated for the federal legislature's regulation of the management of unknown vulnerabilities (*zero-days*) and of the use of external spyware capabilities (Part D.).

---

[9] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 48-66 (*IT-Sicherheitslücken*).

B. Constitutional Requirements for State Vulnerability Management

Does the *Grundgesetz* impose constitutional requirements governing the state's handling of IT vulnerabilities and external spyware capabilities? If so, what are those requirements? To answer these questions, this chapter first identifies the fundamental rights affected by the state's handling of IT vulnerabilities (I.) and examines how state knowledge of vulnerabilities influences the intensity of resulting interferences with those rights (II.). It then argues that the *Grundgesetz* gives rise to a constitutional duty to regulate vulnerability management (III.), which establishes minimum requirements for any such regulatory framework (IV.) while otherwise leaving the legislature a margin of discretion (V.). The procurement of commercial spyware capabilities and the acquisition of such capabilities from allied third states are addressed separately (VI.).

I. Affected Fundamental Rights

The authorities' handling of unknown IT vulnerabilities may interfere with the guaranteed scope of various fundamental rights. The specific doctrinal structures, protective content, and justification requirements of these fundamental rights are therefore central to the constitutional assessment of vulnerability management. In a first step, the fundamental rights affected are therefore briefly presented in outline below. This overview must not, however, obscure the fact that the fundamental rights actually affected, as well as the nature and severity of their impairment, always depend on the specific facts under consideration. Whether, for instance, Art. 10 Grundgesetz is impaired depends on whether a specific vulnerability can also be used to extract communications data, and on whether the specific authority that has knowledge of the vulnerability is permitted (legally), able (technically), and willing (in fact) to use it for communications surveillance. Moreover, the divergences that arise from different fundamental-rights impacts must not be

overstated: the *Bundesverfassungsgericht*, too, operates — particularly in the field of state surveillance — with requirements that cut across fundamental rights.[10]

1. Applicable Fundamental-Rights Regime

Before individual fundamental rights can be considered, the question of the applicable fundamental-rights regime must be clarified. Do only the fundamental rights of the Grundgesetz apply, or only those of the Charter of Fundamental Rights of the European Union, or do both fundamental-rights regimes even apply in parallel?

According to the case law of the Bundesverfassungsgericht, the fundamental rights of the Grundgesetz apply where the norms under review do not serve exclusively to implement mandatory EU law — that is, where they are not fully determined by EU law.[11] This is the case neither for the various security authorities' existing investigative and interference powers[12] nor, as will be shown in Part C.,[13] would it be the case for rules on vulnerability management still to be created.[14] The fact that provisions of EU law have connections to the question of vulnerability management and may already today impose

---

[10] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 125 (*Trojaner I*) (with further references).

[11] BVerfG, Order of 27 May 2020 - 1 BvR 1873/13, 1 BvR 2618/13, Rn. 83-84 (*Bestandsdatenauskunft II*).

[12] See also BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 125 (*Trojaner I*) (PolGNRW); BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 168 (*Trojaner II*) (StPO); BVerfG, Order of 8 October 2024 - 1 BvR 1743/16, 1 BvR 2539/16, Rn. 77-81 (*BND-Cybergefahren*) (G10-Gesetz); BVerfG, Decision of 26 April 2022, Rn. 142-143 (*Bayerisches Verfassungsschutzgesetz*) (BayVfSchG).

[13] Infra C.II.

[14] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18 - 1 BvR 2771/18, Rn. 23 (*IT-Sicherheitslücken*).

requirements on individual authorities regarding the handling of IT vulnerabilities[15] does not preclude this.[16]

Nor does the Charter of Fundamental Rights of the European Union apply in parallel to the constellations of interest here. Under Art. 51(1) CFR, the Charter applies „to the Member States only when they are implementing Union law". Whether such implementation of EU law is present is assessed, according to the case law of the CJEU, in particular by reference to „whether that national legislation is intended to implement a provision of EU law".[17] This is not the case for the constellations and legal matters affected here, as will likewise be shown in Part C.[18]

A different assessment might, of course, be warranted if EU rules were to be enacted.

Alongside the Grundgesetz, the European Convention on Human Rights also always applies; its requirements are to be observed in the interpretation and application of the German fundamental rights.[19]

2. Fundamental Right to the Confidentiality and Integrity of IT Systems, Art. 2(1) in conjunction with Art. 1(1) Grundgesetz

Of particular importance for the debate on state vulnerability management is the fundamental right to the guarantee of the confidentiality and integrity of

---

[15] Infra C.II.

[16] See also BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 23 (*IT-Sicherheitslücken*); See also BVerfG, Judgment of 26 April 2022 - 1 BvR 1619/17, Rn. 142 (*Bayerisches Verfassungsschutzgesetz*); BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 83 (*Trojaner I*); BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 168 (*Trojaner II*); BVerfG, Order of 8 October 2024 - 1 BvR 1743/16, 1 BvR 2539/16, Rn. 77-81 (*BND-Cybergefahren*).

[17] CJEU, Judgment of 10 June 2014, Rs. C-198/13, Rn. 37 (*Julian Hernández ua*); CJEU, Judgment of 22 January 2020, Rs. C-177/18, Rn. 59 (*Baldonedo Martín*).

[18] Infra C.II.

[19] BVerfG, Order of 14 October 2004 - 2 BvR 1481/04, Rn. 32 (*EGMR-Entscheidungen*).

information-technology systems under Art. 2(1) in conjunction with Art. 1(1) Grundgesetz (the IT-system fundamental right).

The IT-system fundamental right — recognized by the Bundesverfassungsgericht in the „Online-Durchsuchungen" decision of 2008 as a special manifestation of the general right of personality[20] — protects the confidentiality and integrity of IT systems that can hold a data subject's data to such an extent and in such variety that access to the system permits insight into significant parts of a person's conduct of life, or even a meaningful picture of their personality.[21]

What is protected here is not only the confidentiality and integrity of the data stored on an IT system covered by the scope of the fundamental right. Rather, the fundamental right shifts protection forward to „the abstract expectation of confidentiality of an IT system before specific data collection processes occur[, because] the process of accessing the system in itself gives rise to specific risks for the data created, processed and stored within or accessible through the system".[22]

The scope of the fundamental right is therefore already impaired when unauthorized persons gain access to a protected IT system; an actual outflow of data or an act of spying is not required.[23] A further precondition, however, is always that the IT system concerned is used as one's own.[24]

Even where state measures also lead to an outflow of data and thereby affect further fundamental rights — in particular Art. 10 Grundgesetz or the right to

---

[20] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 166 ff. (*Online-Durchsuchungen*).

[21] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 97 (*Trojaner I*).

[22] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 100 (*Trojaner I*).

[23] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 100 (*Trojaner I*).

[24] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 104 (*Trojaner I*) (for personally used devices).

informational self-determination — the IT-system fundamental right does not recede behind these.[25]

The state's holding in reserve and keeping secret of IT vulnerabilities can — irrespective of the specific positive obligations the Bundesverfassungsgericht has derived from the fundamental right[26] — interfere with the expectation of confidentiality and integrity protected by the IT-system fundamental right. By leaving known vulnerabilities unpatched, a situation of danger persists that enables unauthorized access to information-technology systems and thereby touches the scope of the fundamental right. The only precondition in this respect is that the vulnerabilities are IT vulnerabilities that actually permit far-reaching access to IT systems sufficiently close to the personality (in particular PCs and mobile phones). For the vulnerabilities at issue here, which often enable very extensive access up to and including root access, this will regularly be the case.

3. Fundamental Right to Telecommunications Privacy, Art. 10 Grundgesetz

The privacy of telecommunications under Art. 10 Grundgesetz likewise plays a role in the constitutional assessment of state vulnerability management.

Art. 10 Grundgesetz protects the incorporeal transmission of information by means of telecommunications traffic, „regardless of the method of transmission (cable or wireless, analogue or digital) and the form of expression (speech, images, sound, symbols or other data) used ”.[27]

---

[25] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 105-118 (*Trojaner I*) (on the relationship between the fundamental right to the confidentiality and integrity of IT systems and Art. 10 Grundgesetz); accordingly superseding BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 27-29 (*IT-Sicherheitslücken*), where it was assumed that state access in the form of source telecommunications surveillance would be subject solely to review under Art. 10 Grundgesetz.

[26] Infra B.III.1.

[27] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 182-183 (*Online-Durchsuchungen*).

Accordingly, in addition to telephony and messaging over mobile networks, internet-based communications services are also protected.[28] The protection covers both the content of communications and the circumstances of communications (such as metadata).[29]

In its „Trojaner I" decision, the Bundesverfassungsgericht held in 2025 that Art. 10 Grundgesetz also applies where the issue is not the transmission of information to individual recipients but „other data transmitted across distances by means of telecommunications technology ", such as data transmitted when accessing websites or otherwise uploading or downloading content.[30]

In the end, the privacy of telecommunications thus protects the entire raw data stream transmitted by telecommunications.[31] Not covered, however, is data skimmed from a data subject's sphere of control outside an ongoing communication process.[32] This does not, however, exclude access to the content of telecommunications from an infiltrated device.[33] Indeed, the Bundesverfassungsgericht goes further and assumes that access to an IT system for the purpose of monitoring ongoing communications is already covered by Art. 10 Grundgesetz.[34]

Analogously to the impairment of the IT-system fundamental right, the holding and keeping-secret of IT vulnerabilities therefore also affects the privacy of telecommunications, since it enables third-party access to the content and circumstances of ongoing telecommunications, which (where the

---

[28] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 183 (*Online-Durchsuchungen*).

[29] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 88 (*Trojaner I*).

[30] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 91 (*Trojaner I*).

[31] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 91 (*Trojaner I*).

[32] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 88 (*Trojaner I*).

[33] See only BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 94 (*Trojaner I*).

[34] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 117 (*Trojaner I*).

state is responsible) constitutes an interference with Art. 10 Grundgesetz. This accords with the Bundesverfassungsgericht's dictum that Art. 10 „requires the state to protect individuals from private third parties gaining access to communications that are protected by the privacy of telecommunications".[35]

4. Fundamental Right to Informational Self-Determination, Art. 2(1) in conjunction with Art. 1(1) Grundgesetz

Third, the state's stockpiling of IT vulnerabilities also affects, in a particular way, the right to informational self-determination, which the Bundesverfassungsgericht derived from the general right of personality under Art. 2(1) in conjunction with Art. 1(1) Grundgesetz.[36]

This right „confers upon the individual the authority to, in principle, decide themselves when and to what extent they wish to disclose personal matters".[37] In principle, it is „affected whenever personal data is collected, stored, used or shared ",[38] regardless of the quantity, quality, sensitivity, or storage location of the data concerned.

As the Bundesverfassungsgericht clarified in its „Trojaner II" decision in June 2025, the right moreover „not only protects against individual instances of data collection, but also against access to large, and thus typically highly informative, datasets".[39] The right to informational self-determination is therefore already impaired by the infiltration of „comprehensive data sets ",

---

[35] BVerfG, Order of 9 October 2002 - 1 BvR 1611/96, 1 BvR 805/98, Ls. 2 (*Mithörvorrichtung*); BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Ls. 1 (*IT-Sicherheitslücken*); further on the protective duty referred to in this context, infra B.III.1.

[36] Foundationally BVerfG, Judgment of 15 December 1983 - 1 BvR 209/83 (*Volkszählung*).

[37] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 223 (*Trojaner II*).

[38] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 223 (*Trojaner II*).

[39] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 223 (*Trojaner II*).

for example the storage of a mobile phone.[40] Moreover, the right to informational self-determination, too, has an inherent protective dimension from which positive obligations may arise.[41]

Where access to an IT system for the purpose of spying out data is concerned, the right to informational self-determination is, according to the case law of the Bundesverfassungsgericht, displaced by the IT-system fundamental right.[42] This applies, however, only insofar as the IT-system fundamental right actually applies — that is, in particular, where the IT system is self-used and sufficiently qualified.[43] The right to informational self-determination can therefore claim validity, for instance, in respect of third parties' communications data stored on an IT system, since here Art. 10(1) Grundgesetz, as a special guarantee, cannot be affected either.[44]

For this reason, it is conceivable that access to an IT system — or the enabling of access to IT systems through the holding of IT vulnerabilities — impairs the right to informational self-determination where, as will often be the case, extensive third-party data is also stored on that system.

5. Further Fundamental Rights of IT Users

IT vulnerabilities, and the attacks they enable, can have very different consequences for the individuals or institutions affected. The risks to the

---

[40] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 223-224 (*Trojaner II*).

[41] BVerfG, Order of 17 July 2013 - 1 BvR 3167/08, Rn. 19 f. (Versicherungsrecht) „The protective duty arising from the right to informational self-determination requires the state to ensure that individuals are in fact able to protect their personal data autonomously.”.

[42] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 227-230 (*Trojaner II*).

[43] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 230 (*Trojaner II*).

[44] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 230 (*Trojaner II*) „In this respect, however, the protection afforded by the right to informational self-determination cannot extend beyond that guaranteed by the fundamental right to the confidentiality and integrity of IT systems”.

freedom and security of individuals thereby addressed[45] may, in the individual case, also be covered by other fundamental rights.[46] Where a cyberattack causes the failure of a hospital's central IT infrastructure, for example, the right to life and physical integrity under Art. 2(2) sentence 1 Grundgesetz may be affected. In the case of ransomware attacks, in which IT systems are paralyzed or encrypted in order to extort a ransom, the guarantee of property under Art. 14(1) Grundgesetz may be affected. Where the infiltration of an IT device is exploited to surveil the affected person's home, an impairment of the inviolability of the home under Art. 13(1) Grundgesetz comes into consideration.[47]

Since these are special liberty rights, a concurrence of fundamental rights with the likewise impaired IT-system fundamental right will, as a rule, have to be assumed here.[48]

Admittedly, a legally relevant impairment of these fundamental rights will, as a rule, occur only through the exploitation of a vulnerability, and not already through the mere compromise of an IT system.[49] In particular, as regards the question of the constitutional permissibility of the state's failure to take protective measures, the impairments mentioned are thus rather abstract risks which, although they must be factored into the constitutional assessment, are not in themselves capable of triggering specific positive obligations or duties to act on the part of the state.

---

[45] See also BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 37 (*IT-Sicherheitslücken*).

[46] Wischmeyer, Informationssicherheit, 2023, p 4 f.; For a comprehensive discussion of this issue, and in particular of the question whether and to what extent specific fundamental rights are affected by the mere compromise of an IT system, see also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 131-137, 197-203.

[47] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 131.

[48] Supra B.I.2.

[49] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 131-137.

6. Fundamental Rights of Vendors

Finally, keeping IT vulnerabilities open may also have effects on the fundamental rights of the vendors of the affected IT components.

Whether the failure to report discovered vulnerabilities interferes with the freedom to choose and practise an occupation under Art. 12(1) Grundgesetz, however, appears doubtful. Here there is presumably a lack of the requisite „occupational nexus“, or of any „occupation-regulating tendency“ as required under German constitutional law.

In any event, an impairment of the general freedom of action under Art. 2(1) sentence 1 Grundgesetz comes into consideration.

II. Severity of the Interference and the Significance of the State's Knowledge and Use of IT Vulnerabilities

The legislature's duty to regulate the state's handling of unknown IT vulnerabilities[50] ultimately rests on a simple insight: keeping unknown IT vulnerabilities open produces specific consequences burdening fundamental rights that carry considerable weight in fundamental-rights terms and are independent of the exploitation of a vulnerability. These consequences alone are so grave that, from a constitutional standpoint, they must be answered for at the parliamentary level and thus make legislative intervention necessary.[51]

First and foremost, it must be borne in mind that unknown IT vulnerabilities regularly pose the most serious IT security risks for users of the affected IT infrastructure.[52] There is regularly a state interest in keeping open precisely those vulnerabilities that enable especially far-reaching access to others' IT systems and are therefore suitable for infiltration or manipulation purposes.

---

[50] Infra III.

[51] On the various legal bases for such intervention, infra B.III.

[52] See also BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 36-37 (*IT-Sicherheitslücken*).

Via such vulnerabilities it is normally possible both to spy out the entire data holdings of an infiltrated device and to alter and manipulate it. What is then possible is thus not only the spying-out of even the most sensitive information and records — such as intimate chat histories, banking data, or health information — and, bound up with this, the gravest endangerment of the affected persons' personality rights, but also attacks such as the encryption of the data found, of the kind used in so-called ransomware attacks.[53] Yet precisely such powerful vulnerabilities are of interest not only to state bodies. Rather, they also constitute attractive attack vectors for criminal actors, as well as for foreign security authorities, which are known to deploy such vulnerabilities in part without a sufficient legal basis. Where the state does not work towards closing such vulnerabilities, it must therefore reckon with their being exploited by any third party, causing harm to holders of fundamental rights.[54] This applies in particular where the state has not discovered the vulnerability itself but has obtained knowledge of it from third parties — for instance, from third states or on the grey or black market.

Closely bound up with this is the fact that vulnerabilities often affect an indeterminate multitude of IT users[55] and that keeping them open therefore gives rise to risks with a considerable spread.[56] The absolute majority of those affected have never given, and never will give, occasion for measures by security authorities, yet are nonetheless exposed to profound endangerment of the IT infrastructure they use.[57]

---

[53] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 37 (*IT-Sicherheitslücken*).

[54] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, p 65 („Kollisionsrisiko").

[55] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 239-241 (*Online-Durchsuchungen*); BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 193 (*Trojaner II*).

[56] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 119-120.

[57] On the criteria of the number of affected fundamental rights holders and the measure's linkage to a specific cause: BVerfG, Judgment of 14 July 1999 - 1 BvR 2226/94, Rn. 219 (*Telekommunikationsüberwachung I*); BVerfG, Judgment of 2 March 2010 - 1 BvR 256/08, Rn. 210 (*Vorratsdatenspeicherung*); BVerfG, Order of 27 May 2020 - 1 BvR 1873/13, 1 BvR 2618/13 - 1 BvR 1873/13, Rn. 129 (*Bestandsdatenauskunft II*).

Added to this is the fact that individuals — private persons as well as companies and other institutions — cannot, as a rule, protect themselves against *zero-day* vulnerabilities.[58] In any event, (effective) informational self-protection presents considerable difficulties and entails great effort and cost.[59]

It must further be taken into account that the state's stockpiling of knowledge about unknown IT vulnerabilities can carry a considerable risk of loss, in that the „central" storage of such information constitutes a particularly coveted target of attack for third parties.[60] The risk that secret knowledge of IT vulnerabilities reaches third parties through infiltration or cyberattacks is, as history shows, anything but theoretical: in 2016, for example, the hacker group „Shadow Brokers" announced that it had stolen zero-day exploits from the National Security Agency (NSA). Shortly afterwards, one of these exploits was used in the global ransomware campaign „WannaCry", which put hundreds of thousands of computers out of operation and caused damage of nearly £100 million to the British health system, the NHS, alone.[61]

Beyond this, every vulnerability carries a risk of misuse: it technically enables the security authorities that possess it to do more than they are legally permitted to do.[62] This concerns, on the one hand, the technical potential of the vulnerability in the context of a planned and permissible deployment. For normally, the breadth of interference made possible by a given vulnerability

---

[58] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 37 (*IT-Sicherheitslücken*).

[59] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 180 (*Online-Durchsuchungen*); Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 116-117.

[60] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, p 65-66.

[61] National Health Executive, „*WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled*" (12. Oktober 2018) https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled.

[62] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, p 66.

exceeds what is legally permissible.[63] On the other hand, it must also be taken into account that officials may misuse vulnerabilities for entirely unauthorized deployments. This risk, too, arises already with knowledge of an unknown and unpatched vulnerability and is independent of the statutory powers to use vulnerabilities.

To these concrete dangers, arising from knowledge of the individual vulnerability, are added structural risks whose fundamental-rights-impairing effect need be no less grave:

As the Bundesverfassungsgericht already set out in the *Online-Durchsuchung* decision, *zero-day* vulnerabilities give rise to a dilemma for the state: the interest in the highest possible IT security conflicts with the interest in exploiting the vulnerability and in the secrecy this entails.[64] In this respect, the dilemma can "undermine the public's confidence that the state is committed to ensuring the highest possible security of information technology"[65] and thereby inhibit users in the exercise of their liberty rights in the digital space. Particularly for actors who wish to communicate especially sensitive data — such as members of the opposition, journalists, but also state institutions — the *chilling effects*[66] thereby addressed can be palpable.

The potential use of unknown vulnerabilities by state authorities further creates an incentive for security researchers not to report identified vulnerabilities to the affected vendors, so as to be able to sell them instead to state purchasers.[67] As the primary purchasers of *zero-day* exploits, state

---

[63] This is the case because such access typically entails unrestricted read and write permissions to the compromised system.

[64] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 241 (*Online-Durchsuchungen*).

[65] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 241 (*Online-Durchsuchungen*).

[66] Generally regarding *chilling effects* auch BVerfG, Judgment of 2 March 2010 - 1 BvR 256/08, Rn. 212 (*Vorratsdatenspeicherung*).

[67] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 42 (*IT-Sicherheitslücken*).

actors are in fact chiefly responsible for the emergence of the market for such vulnerabilities[68] and thus contribute significantly to the emergence and persistence of considerable IT security risks.

III. Constitutional Foundations of a Statutory Duty of Vulnerability Management

The constitutional duty to enact statutory rules on the state's handling of IT vulnerabilities rests on three constitutional foundations that apply in parallel: first, it is necessary in order to fulfil the state's positive obligations derived from the IT-system fundamental right and the privacy of telecommunications (1.). It further follows from the requirement of parliamentary legislation and the essential-matters doctrine (2.) and from the principle of proportionality (3.).

1. Vulnerability Management and the Fundamental-Rights-Based Duty to Protect

As early as 2002, the Bundesverfassungsgericht held, in its decision on eavesdropping devices,[69] that a state protective mandate follows from Art. 10 Grundgesetz to safeguard telecommunications against access by private third parties.[70] This protective mandate is grounded in the particular susceptibility of telecommunications to such unauthorized access.[71]

---

[68] See also B.VI.1.a).

[69] In the two proceedings at issue, third parties had each intercepted a telephone conversation via the speakerphone function built into standard landline telephones.

[70] BVerfG, Order of 9 October 2002 - 1 BvR 1611/96, 1 BvR 805/98, Rn. 21 (*Mithörvorrichtung*).

[71] BVerfG, Order of 9 October 2002 - 1 BvR 1611/96, 1 BvR 805/98, Rn. 20 (*Mithörvorrichtung*).

In its „IT-Sicherheitslücken" decision of June 2021,[72] which concerned a 2017 authorization for source telecommunications surveillance (Quellen-TKÜ) in the Baden-Württemberg Police Act, the Court then concretized this protective mandate into a fundamental-rights positive obligation.[73]

The complainants had objected here that the authorization to use source telecommunications surveillance would have the consequence that police authorities would not report *zero-day* vulnerabilities known to them to the vendors but would instead keep them open in order to exploit them for infiltration purposes.[74] This would also enable attacks by third parties.[75] The incentive triggered by that power not to report IT vulnerabilities to the affected vendors therefore amounted to a violation of the state's positive obligation derived from the objective-law dimension of the IT-system fundamental right.[76] That obligation could be fulfilled only by an accompanying rule on vulnerability management — one that must be anchored in statute — which would have to provide for a regulated procedure for assessing and deciding on *zero-day* vulnerabilities.[77]

The Bundesverfassungsgericht essentially confirmed this reasoning and affirmed a specific state positive obligation: where state authorities know of a vulnerability unknown to the vendors, the state is obliged to protect the users of information-technology systems against third-party attacks on those systems.[78] This follows from the protective dimension arising from Art. 10(1)

---

[72] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 26 ff. (*IT-Sicherheitslücken*).

[73] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 26 (*IT-Sicherheitslücken*).

[74] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 4 (*IT-Sicherheitslücken*).

[75] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 4 (*IT-Sicherheitslücken*).

[76] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 9 (*IT-Sicherheitslücken*).

[77] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 10 (*IT-Sicherheitslücken*).

[78] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 26 (*IT-Sicherheitslücken*).

Grundgesetz and the IT-system fundamental right applicable here in concurrence.[79]

This protective dimension is grounded in the insight that citizens today depend on the use of networked information technology in order to exercise their constitutionally protected freedom of self-development, and can therefore ever less evade the dangers of this use.[80] For this reason, the state is „obliged to help protect the integrity and confidentiality of IT systems from third-party attacks".[81]

Where the state knows of vulnerabilities that are unknown to vendors 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".[82] This positive obligation rests on three grounds: first, IT vulnerabilities carry a high potential for endangerment and harm — and not only to the privacy of citizens, but also, for instance, to businesses and to commercial trade in general.[83] Second, individuals are generally unable to protect themselves effectively against the dangers of unknown vulnerabilities.[84] Third, in the cases covered there is a special protective obligation on the part of the state, because the state — unlike the vendors and users of the infrastructure — has knowledge of the vulnerability.[85]

---

[79] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 33 (*IT-Sicherheitslücken*).

[80] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 33 (*IT-Sicherheitslücken*).

[81] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 33 (*IT-Sicherheitslücken*); for a comprehensive discussion of the grounds for a state duty to protect IT security, see also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 176-185.

[82] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 34 (*IT-Sicherheitslücken*).

[83] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 36-38 (*IT-Sicherheitslücken*).

[84] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 39 (*IT-Sicherheitslücken*).

[85] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 40 (*IT-Sicherheitslücken*).

This positive obligation does not, admittedly, preclude the use of vulnerabilities for infiltration purposes, but it requires the legislature to enact „a legal framework that governs how [authorities], when deciding on keeping unknown security vulnerabilities open, [are] 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".[86]

Specifically, authorities „must be required to balance these conflicting interests".[87] In this regard, 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".[88]

In the end, the Bundesverfassungsgericht allowed the constitutional complaint to fail on the ground that the complainants had not satisfied the special constitutional pleading requirements that must be met in order to substantiate a breach of a positive obligation.[89] For since the Bundesverfassungsgericht can find a breach of a positive obligation only „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",[90] establishing even the possibility of a fundamental-rights violation requires complainants to „address the entire legislative context, which requires – depending on the

---

[86] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 44 (*IT-Sicherheitslücken*); see also Rn. 34, 41-43.

[87] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 44 (*IT-Sicherheitslücken*).

[88] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 44 (*IT-Sicherheitslücken*).

[89] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 48-66 (*IT-Sicherheitslücken*).

[90] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 50 (*IT-Sicherheitslücken*) (established case law).

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”.[91]

The complaint would accordingly have had to engage, on the one hand, with the clause contained in the authorizing power at issue on the „protection of the used tool against misuse”, and, on the other, with various provisions of police, data-protection, and cybersecurity law and with the sub-statutory reporting standard of the IT-Planungsrat[92].[93] To observe the principle of subsidiarity, the complainants would moreover have had to attempt to have questions of interpretation regarding these provisions resolved by the specialized courts.[94]

The existence of a concretized state positive obligation requiring the state to regulate the handling of IT vulnerabilities was affirmed in the decisions „Hessentrojaner”,[95] „Bayerisches Verfassungsschutzgesetz”,[96] „Trojaner I”,[97] and „Trojaner II”.[98] In these decisions, too, however, the Court considered the admissibility requirement of sufficient substantiation of a breach of a positive obligation not to be met, since the complainants — again in line with the standard mentioned — had not sufficiently shown that, taking

---

[91] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 51 (*IT-Sicherheitslücken*).

[92] IT-Planungsrat, Verbindliches Meldeverfahren zum Informationsaustausch über Cyberangriffe (5.10.2017), https://www.it-planungsrat.de/fileadmin/beschluesse/2017/Beschluss2017-35_Meldestandards_Anlage1.pdf.

[93] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 53-66 (*IT-Sicherheitslücken*).

[94] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 67-74 (*IT-Sicherheitslücken*).

[95] BVerfG, Order of 20 January 2022 - 1 BvR 1552/19, Rn. 17 (*Hessentrojaner*).

[96] BVerfG, Judgment of 26 April 2022 - 1 BvR 1619/17, Rn. 111 (*Bayerisches Verfassungsschutzgesetz*).

[97] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 51-53 (*Trojaner I*).

[98] BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 108 (*Trojaner II*).

the statutory regulatory context into account, one could assume a failure of the legislative scheme.[99]

The Bundesverfassungsgericht's restraint is understandable not only on procedural grounds. In the democratic constitutional state, it is primarily for the legislature to counteract dangers to fundamental rights. In doing so, it is in principle also accorded latitude for assessment, evaluation, and design.[100] However, the fact that the Bundesverfassungsgericht, in its settled case law, is prepared to find a *breach* of a positive obligation only „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“,[101] does not cause the legislature's objective legal obligation to comply with its positive obligation to fall away. The legislature must thus, as a matter of constitutional law, act comprehensively in the interest of fundamental-rights protection, even if not every falling-short of constitutional expectations is directly justiciable.

The fact that the Bundesverfassungsgericht, in the *IT-Sicherheitslücken* decision, not only affirmed the existence of a fundamental-rights positive obligation for IT security — that is, a specific objective-law binding of the parliamentary legislature — but at the same time concretized this obligation towards the statutory anchoring of a vulnerability-management process,[102] can and must therefore be understood as an explicit call on the legislature to act in this direction.

---

[99] BVerfG, Order of 20 January 2022 - 1 BvR 1552/19, Rn. 17 (*Hessentrojaner*).; BVerfG, Judgment of 26 April 2022 - 1 BvR 1619/17, Rn. 111 (*Bayerisches Verfassungsschutzgesetz*); BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 52-53 (*Trojaner I*); BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 108 (*Trojaner II*).

[100] BVerfG, Order of 24 March 2021 - 1 BvR 2656/18, Rn. 152 (*Klimaschutzgesetz*) (m.w.N).

[101] BVerfG, Order of 24 March 2021 - 1 BvR 2656/18, Rn. 152 (*Klimaschutzgesetz*) (m.w.N).

[102] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 189-190.

This mandate is urgent, for the statutory provisions cited by the Bundesverfassungsgericht as potentially relevant to fulfilling the positive obligation plainly do not, on thorough analysis, constitute protective precautions that meet the Court's requirements.[103] Nor can any sufficient protective concept be derived — as will in part be shown in Part C. — from other regulatory instruments, some of which entered into force after the *IT-Sicherheitslücken* and *Bayerisches Verfassungsschutzgesetz* decisions, in particular the revised BSI Act, the Cyber Resilience Act, and the Cybersecurity Act.[104] At present, it must therefore be stated that the existing statutory framework is probably in fact wholly unsuitable and entirely inadequate to fulfil the positive obligation derived from the IT-system fundamental right,[105] and that fulfilment of the duty to enact statutory rules on vulnerability management remains outstanding.

2. Vulnerability Management and the Essential-Matters Doctrine

The constitutionally grounded requirement of parliamentary legislation and the closely intertwined essential-matters doctrine likewise argue strongly in favour of the constitutional necessity of anchoring vulnerability management in statute.

In its settled case law, the Bundesverfassungsgericht derives from the rule-of-law principle and the democratic principle the legislature's duty „to make the essential decisions itself in all fundamental normative areas".[106] The legislature is therefore, in particular, obliged „to make the regulations

---

[103] Wischmeyer, *Informationssicherheitsrecht*, 2023, p 290-292; Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 237-257.

[104] Infra C.II.

[105] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 258 (with further references).

[106] BVerfG, Judgment of 19 September 2018 - 2 BvF 1/15, 2 BvF 2/15, Rn. 191 (*Zensus 2011*) (established case law).

essential for the realization of fundamental rights substantially itself, and not to leave these to the actions and decision-making power of the executive”.[107] The requirement of parliamentary legislation is intended to ensure that fundamental political decisions are taken in a transparent, democratic discourse and that account is publicly rendered for the necessity and extent of interferences with fundamental rights.[108]

What counts in this respect as essential to fundamental rights, and thus to be answered for by the legislature, has been outlined by the Constitutional Court only rudimentarily. Decisive, first, is „the significance of the subject matter of the regulation and the intensity of the interferences with fundamental rights effected by or on the basis of the regulation”.[109] A duty to intervene legislatively „exists in particular in multidimensional, complex fundamental-rights constellations in which competing liberty rights meet one another and whose respective boundaries are fluid and difficult to determine".[110] „When and to what extent regulation by the legislature is required can however only be determined with regard to the particular subject area and the specific nature of the regulatory subject matter concerned”.[111]

The essential character of a matter then decides not only the question of *what* must be regulated by the legislature itself, but also *to what extent* and *with what degree of specificity*.[112] The more essential the questions to be decided,

---

[107] BVerfG, Order of 21 April 2015 - 2 BvR 1322/12, 2 BvR 1989/12, Rn. 53 (*Altershöchstgrenzen*) (established case law).

[108] BVerfG, Order of 21 April 2015 - 2 BvR 1322/12, 2 BvR 1989/12, Rn. 53 (*Altershöchstgrenzen*).

[109] BVerfG, Judgment of 19 September 2018 - 2 BvF 1/15, 2 BvF 2/15, Rn. 196 (*Zensus 2011*).

[110] BVerfG, Oder of 21 April 2015 - 2 BvR 1322/12, 2 BvR 1989/12, Rn. 53 (*Altershöchstgrenzen*); BVerfG, Judgment of 19 September 2018 - 2 BvF 1/15, 2 BvF 2/15, Rn. 194 (*Zensus 2011*).

[111] BVerfG, Judgment of 19 September 2018 - 2 BvF 1/15, 2 BvF 2/15, Rn. 193 (*Zensus 2011*) (established case law).

[112] BVerfG, Judgment of 19 September 2018 - 2 BvF 1/15, 2 BvF 2/15, Rn. 196 (*Zensus 2011*) (established case law).

the more extensive and denser the legislative regulation must be. Only in this way is an effective limitation and steering of the administration, and effective review by the courts, possible.[113] The complexity or openness to development of a particular regulatory field may, however, militate against a particularly detailed legislative design.[114]

Measured against these standards, the following good reasons support assuming a fundamental-rights duty to enact legislative rules on the handling of IT vulnerabilities:[115] as already shown, the handling of IT vulnerabilities has extensive effects on various fundamental rights.[116] This applies not only to the use of a vulnerability but, owing to the risks addressed above,[117] already to the decision whether to keep a vulnerability open, as is also expressed in the *IT-Schwachstellen* decision. This decision alone is therefore, for the reasons stated, already significant for fundamental rights.

It constitutes, in that respect, a „multidimensional, complex fundamental-rights constellations" in which the frictions between the various conflicting fundamental rights and constitutional values are difficult to determine. It is precisely this complexity and conflict-laden character of the fundamental-rights positions affected that suggests reserving the requisite balancing decisions to the parliamentary legislature. For the decision whether to keep open or report an IT vulnerability is not merely a matter of technical or operational questions of threat prevention, but concerns fundamental value judgments about the relationship between state security interests, the IT security of the general public, and the liberty rights of those affected. Such decisions touch central questions of securing freedom in the digital space and

---

[113] BVerfG, Judgment of 19 September 2018 - 2 BvF 1/15, 2 BvF 2/15, Rn. 196 (*Zensus 2011*) (established case law).

[114] BVerfG, Judgment of 19 September 2018 - 2 BvF 1/15, 2 BvF 2/15, Rn. 196 f. (*Zensus 2011*).

[115] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 195-197.

[116] Supra B.I.

[117] Supra B.II.

therefore require democratically legitimated regulation, publicly answered for, by the legislature.

Added to this is the fact that the handling of unknown IT vulnerabilities is, by its nature, marked by structural opacity. Decisions about stockpiling, using, or disclosing vulnerabilities are regularly taken within the executive and, owing to the need for secrecy, are subject to only very limited public scrutiny. Precisely under such conditions, it falls to the parliamentary legislature to lay down, through statutory requirements, decision-making procedures, balancing criteria, and control mechanisms, in order to ensure a limitation of executive latitude that is sufficient in rule-of-law terms. These aspects, too, support the view that the decisive guiding choices may not be left to the administration but must be made by way of parliamentary legislation.[118]

3. Vulnerability Management and the Principle of Proportionality

As already discussed, the state's handling of IT vulnerabilities can have (negative) effects on the exercise of fundamental rights in manifold ways and, where the threshold of an interference with fundamental rights is reached, may be relevant to the defensive dimension of fundamental rights. The exploitation of vulnerabilities for infiltration purposes, for instance, clearly constitutes an interference with fundamental rights. But the purchasing, researching, holding, or sharing of vulnerabilities may already impair fundamental rights, in particular the IT-system fundamental right.

Irrespective of the question which of these activities specifically crosses the threshold of an interference with fundamental rights, this defensive perspective raises the question of the proportionality of vulnerability-related state actions. In corresponding constellations, the principle of proportionality is regarded by the Bundesverfassungsgericht, too, as a central standard for the justification of interferences with fundamental rights protecting the right

---

[118] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 195-197.

of personality.[119] A statutory duty of vulnerability management would, for all vulnerability-related state activities, contribute to securing precisely this proportionality, and could in certain situations even be indispensable.

This follows from the function of vulnerability management for the proportionality assessment: the central parameter of that assessment is, first, the severity of the interference.[120] As already shown,[121] the Bundesverfassungsgericht, too, has repeatedly emphasized that the use — and the concomitant keeping-open — of IT vulnerabilities increases the severity of the interferences triggered by security authorities' powers of interference.[122]

In return, statutory rules on the handling of IT vulnerabilities would reduce the weight of corresponding impairments. For such rules would not only procedurally ensure that the usability of a vulnerability can be justified against the background of its potential for harm, but would moreover enable a certain degree of transparency and supervisory control.[123]

Moreover, the Bundesverfassungsgericht holds in settled case law that, in the case of covert surveillance measures, the principle of proportionality imposes requirements as to transparency, individual legal protection, and supervisory control.[124] If — as already noted[125] — one correctly regards even the decision to keep a vulnerability open as significant for fundamental rights, as is also expressed in the IT-Schwachstellen decision, it is natural to transfer these requirements, in principle, to vulnerability management as well. Because,

---

[119] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 124 (*Trojaner I*).

[120] BVerfG, Order of 24 June 2025 - 1 BvR 2466/19, Rn. 124 (*Trojaner I*).

[121] Siehe B.II.

[122] BVerfG, Judgment of 27 February 2008 - 1 BvR 370, 595/07, Rn. 139-142 (*Online-Durchsuchungen*); BVerfG, Order of 24 June 2025 - 1 BvR 180/23, Rn. 193 (*Trojaner II*) f.

[123] See also B.IV.7. und B.V.3.

[124] BVerfG, Judgment of 20 April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Rn. 134 ff. (*BKA-Gesetz*).

[125] Supra B.III.2.

however, transparency and individual legal protection are subject to narrow limits in the case of keeping IT vulnerabilities open — as with the use of covert surveillance methods — supervisory control takes on particular importance in this respect.[126] But control is possible only where a formal decision has been made on the use of a vulnerability and that decision, together with the considerations determining it, has been recorded.[127] Such a binding, uniform, and judicially reviewable duty to decide and to keep records cannot, however, be ensured by mere internal administrative requirements, which the executive could alter at any time and remove from parliamentary as well as judicial control. Since, moreover — as shown — what is at issue are guiding decisions essential to fundamental rights, the legislature is bound to regulate the decisive procedural, balancing, and control requirements itself. Ultimately, this can be achieved only through statutory regulation of vulnerability management.

IV. Constitutional Minimum Requirements

If, in line with the foregoing considerations, one assumes that a legislative duty to regulate the state's handling of IT vulnerabilities follows from the Constitution, the further question arises how this regulation must be designed.

From the case law of the Constitutional Court, as well as from general constitutional considerations, certain minimum requirements for the design of an official duty of IT vulnerability management can be derived (on this, 1.–8. below). For further regulatory aspects, by contrast, the Constitution contains no concrete requirements; in that regard, requirements can be developed only from considerations of appropriate design (on this, II.).

---

[126] BVerfG, Judgment of 20 April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Rn. 140 (*BKA-Gesetz*).

[127] Vgl. auch BVerfG, Judgment of 20 April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Rn. 141 (*BKA-Gesetz*).

1. Regulation by Formal Statute

a) Necessity of a Formal Statute

First, vulnerability management must necessarily be regulated by formal statute and may not be delegated in its entirety to sub-statutory rule-making or administrative procedures.

In the IT-Sicherheitslücken decision, the Bundesverfassungsgericht itself held in this respect: „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".[128]

It cannot be objected to this that the Bundesverfassungsgericht, in its cursory account — given by way of *obiter dictum* — of relevant existing provisions, also referred to the reporting standard adopted by the IT-Planungsrat[129], „Verbindliches Meldeverfahren zum Informationsaustausch über IT-Sicherheitsvorfälle im VerwaltungsCERT-Verbund", and thus to a rule that is neither a formal nor a substantive statute. For, on the one hand, both the duty to establish IT security standards such as the reporting standard and their binding effect are anchored in statute (§ 2(1) and (2) IT-Staatsvertrag, respectively). On the other hand, the Bundesverfassungsgericht itself noted that „[t]he 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".[130] At the same time, it pointed to the other statutory provisions that might come into consideration.

Moreover, the duty to anchor the official duty of vulnerability management in statute also follows from the requirement of parliamentary legislation and the

---

[128] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 41 (*IT-Sicherheitslücken*).

[129] The IT Planning Council is a steering body of the Federation and the Länder that coordinates cooperation in the field of joint information technology established under Article 91c Grundgesetz.

[130] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 66 (*IT-Sicherheitslücken*).

essential-matters doctrine,[131] since the state's decision on the secrecy or disclosure of IT vulnerabilities is, as shown above, essential to the reconciliation of conflicting fundamental rights and constitutional goods and thus, in constitutional terms, essential overall.

b) Scope of the Anchoring in Formal Statute

It is then questionable what degree of detail the regulation of vulnerability management by formal statute — or its anchoring therein — must reach, that is, which regulatory choices may be entrusted to sub-statutory rule-making or to administrative practice.

It is clear, first, that the statutory rules must regulate at least those aspects expressly named by the Bundesverfassungsgericht in the IT-Sicherheitslücken decision as components of the statutory rules to be created,[132] that is, the determination of a balancing process, including the interests to be balanced (on this, 3.), and the fixing of a rule–exception relationship (on this, 4.).

Further, it belongs to the essential content of any vulnerability rules *whom* the duty to decide falls upon *in which cases* (the question of the addressees of the rules, on this, 2.), *who* makes the decision on secrecy or disclosure (the question of decision-making competence, on this, 5.),[133] and which duties to act the decision can trigger (the question of the consequences of the decision, on this, 6.). Finally, the statute must, at least in principle, also provide rules for the protection of vulnerabilities kept secret (on this, 7.) and for the oversight and review of the decision taken (on this, 8.).

Other aspects of the substantive and procedural design of vulnerability management — for instance, more specific requirements on the (standardization of the) selection, weighting, and relation of the interests to

---

[131] Supra B.III.2.

[132] See also supra B.III.1.

[133] As regards decision-making authority, the legislature nevertheless has various regulatory options available (see therefore also B.V.1.).

be balanced, on the design of the decision-making procedure (e.g. allocation of tasks, sub-competences), or on any transparency duties — can, by contrast, be delegated to the authority issuing the ordinance.

2. Addressees and Subject Matter of the Regulation

The first question that statutory rules on vulnerability management must answer is that of the addressees and the scope of the rules: which state institutions are to run an orderly procedure for deciding how to handle which IT vulnerabilities, once they become aware of them?

The aspect of the institutions covered can be derived directly from the *IT-Sicherheitslücken* decision. That decision does not limit the arising of the state positive obligation to particular authorities;[134] all conceivable authorities and state institutions must run the vulnerability-management procedure where they become aware of a covered vulnerability.[135]

Covered, however, are only *zero-day* vulnerabilities, that is, vulnerabilities unknown to vendors. Admittedly, *N-day* vulnerabilities, too, pose considerable security dangers, which are exploited by criminal as well as state actors.[136] But the specific dangers that ground the arising of a state positive obligation under the IT-Sicherheitslücken decision — particularly serious infiltration risks, no possibility of digital self-protection, the state's capacity to act coupled with the affected vendor's incapacity to act — exist in

---

[134] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 35 (*IT*-Sicherheitslücken) „If state authorities become aware of security vulnerabilities, the state’s general duty to protect becomes a concrete constitutional obligation to protect fundamental rights.”.

[135] However, this protective mandate cannot expand the legislative competence of the Federation or the Länder; accordingly, as will be shown below (C.III.), the Federation is only empowered to impose obligations on its own authorities.

[136] See also Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 12.

this way only for unknown vulnerabilities.[137] The vulnerability must therefore be unknown both to the vendor and to the public.[138]

The Bundesverfassungsgericht here draws no distinction between vulnerabilities the state has discovered itself and those it has procured from third parties.[139] Specific questions arising in connection with the acquisition of vulnerabilities from private or state third parties are returned to below.[140]

Further, according to the decision, no limitation of the covered vulnerabilities — for example, by the type of IT infrastructure affected — is indicated either. Where IT systems are used exclusively by state institutions in their function as bearers of public authority, those institutions cannot invoke fundamental rights, so that the constitutional positive obligation is not triggered. It is therefore conceivable that so-called Government off-the-shelf components (GOTS) — that is, software or hardware produced specifically for state use — are excluded from the scope of the positive obligation. Such an exception would, however, appear to be precluded, at any rate on grounds of expediency.[141]

An exception must, however, be made for vulnerabilities transmitted to the state solely for the purpose of coordinated disclosure under the so-called

---

[137] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 35-40 (*IT-Sicherheitslücken*), Rn. 40 „It is precisely this knowledge, combined with the manufacturer's lack of awareness and the affected individuals' inability to protect themselves, that gives rise to the state's heightened duty of protection".

[138] Public knowledge exists where the vulnerability is documented in publicly accessible sources; see also *Vulnerabilities Equities Policy and Process for the United States Government* (*U.S. VEP*) (15.11.2017), abrufbar unter https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/external%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF, p 12.

[139] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 40 (*IT-Sicherheitslücken*).

[140] See also B.VI.

[141] *U.S. VEP* (2017) p 3 „This policy [...] includes Government off-the-shelf (GOTS), Commercial off-the-shelf (COTS), or other commercial information systems (to include open-source software), Industrial Control Systems (ICS) or products, and associated systems such as Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).".

Coordinated Vulnerability Disclosure (CVD) procedure.[142] These vulnerabilities must be reported directly to the affected vendors and may therefore not be fed into the vulnerability-management process.[143] Those who report here rely on the information being used exclusively for forwarding to the affected vendors; state use for its own purposes would break this trust and thereby jeopardize vulnerability reports that are central to society-wide IT security. Moreover, given the existing third-party awareness of the vulnerability, it could not in any event be assumed that the state could successfully exploit it for its own purposes.

In emergencies, too, where a delay in disclosing the vulnerability would trigger serious disadvantages (for example, because the vulnerability is being actively exploited by third parties), the procedure must be dispensed with and the vulnerability immediately directed towards being patched.[144]

3. Balancing Process

Further, the statutory rules must oblige the authorities concerned to carry out a balancing procedure in which the risks and benefits of keeping the vulnerability secret are to be weighed and set against one another.

a) Duty to Balance

The Bundesverfassungsgericht sees no duty to close every vulnerability of which an authority becomes aware: „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

---

[142] Coordinated Vulnerability Disclosure (CVD) processes are procedures through which security researchers can initially report discovered vulnerabilities confidentially to the affected manufacturers or designated coordinating bodies, enabling them to guide remediation before the vulnerability is publicly disclosed. In Germany, the Federal Office for Information Security (BSI) provides a CVD process.

[143] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 18.

[144] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 18; regarding further possible exemptions, *U.S. VEP* (2017) p 10.

claim that authorities must notify developers about any IT security vulnerabilities immediately and in all circumstances.”.[145]

However, „[i]t 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“.[146]

As this very formulation of the Bundesverfassungsgericht indicates, the balancing process need be run through only where the discovering authority wishes to keep the vulnerability open. The reporting of the vulnerability to the affected vendors, by contrast, the authority may initiate on its own responsibility. In doing so, the authority directly complies with its positive obligation for IT security, rooted in the Grundgesetz, which requires no further procedural safeguarding.

b) Interests to Be Balanced

This already touches on the essential interests to be taken into account in this balancing. On the side of the affected IT users, „die Gefahr einer weiteren Verbreitung der Kenntnis von [der] Sicherheitslücke” must in particular be factored in. If the positive obligation serves to ward off unauthorized third-party access, it seems imperative that the analysis determine not only the danger of dissemination of *knowledge* of the vulnerability but also the danger of *use* of the vulnerability and the (fundamental-rights) *potential for harm* thereby enabled, in terms both of extent and of quality. Against these dangers, the „quantitativ und qualitativ” determined benefit of a possible official infiltration via the vulnerability is to be weighed.

---

[145] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 43 (*IT-Sicherheitslücken*).

[146] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 44 (*IT-Sicherheitslücken*).

The factors to be balanced are to be pre-structured by statute;[147] a detailed determination — inspired, for instance, by existing processes[148] — can take place in derived legal acts.

4. Rule–Exception Relationship

Moreover, it follows from the IT-Sicherheitslücken decision that, as a rule, the vulnerability must be reported to the vendor. Only where, in the exceptional case, the interest to keep the vulnerability secret and open, may reporting be omitted.[149] This fixes the fundamental priority of protecting IT security, as also represents the standard in the literature and in foreign vulnerability rules (so-called *default-to-disclose*).[150]

5. Decision-Making Competence and Process

The institutional location and procedural design of vulnerability management have a decisive influence on the interpretation and application of the substantive-law requirements — and thus on fundamental-rights protection as well — and therefore constitute essential elements that must necessarily be determined by the statutory rules themselves.[151]

From the Constitution, however, no entirely concrete requirements as to the institutional design, competence, and procedure of the vulnerability management to be established can be derived. Possible and sensible

---

[147] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, p 76.

[148] For an overview of relevant considerations, see for example *U.S. VEP* (2017) Annex B.

[149] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 44 (*IT-Sicherheitslücken*).

[150] See also *U.S. VEP* (2017) p 1 „the primary focus of this policy is to prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities discovered by the USG, absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, Law Enforcement, or national security purposes.”.

[151] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, p 77.

regulatory options are therefore presented in the section on appropriate design.[152]

6. Consequences of the Decision

Further, the statutory basis of vulnerability management must already lay down which consequences may be chosen among at the end of the process.

The disclosure of the vulnerability by reporting it to the vendor, on the one hand, and keeping the vulnerability secret, on the other, are indeed the two most important, but not the only two, courses of action. As is also set out, for instance, in the VEP, the state may in addition, for example, 1) pass on information that can reduce the risk of exploitation without disclosing the specific vulnerability, 2) restrict in a particular way the use of the vulnerability by state bodies, or 3) confidentially inform domestic and/or foreign authorities about the vulnerability.[153]

The various courses of action should be listed in the statutory basis with sufficient specificity.

Further, the statutory basis must already lay down that a vulnerability kept secret must be periodically re-evaluated until it is ultimately — as is required for every vulnerability[154] — reported. The evaluation cycle and any duties to act upon the occurrence of unforeseen emergency situations can also be laid down in sub-statutory rules.

If the decision goes — as must, as a rule, be the case[155] — against withholding the vulnerability, it must be reported to the vendor in a CVD process. The BSI

---

[152] Infra B.V.1.

[153] *U.S. VEP* (2017) p 1; Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 31-33; For instance, the state can caution operators of critical infrastructure against the unrestricted deployment of certain IT infrastructure without disclosing the discovered vulnerability to either the operators or the manufacturer.

[154] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 14.

[155] See B.IV.4.

should be entrusted with this; it can also be commissioned by private parties to carry out CVD procedures.[156]

7. Oversight and Review

As in other areas of security-service activity, the Grundgesetz requires, for official decisions on keeping IT vulnerabilities open as well, appropriate oversight and control mechanisms exercised by independent and adequately resourced bodies.[157]

The Bundesverfassungsgericht emphasizes in settled case law that the lack of transparency and the extensive limitation of individual legal protection in the case of (covert) surveillance measures must be compensated by special requirements for the independent objective-law review of such measures.[158] In the area of intelligence gathering, it has moreover required that „to compensate for the fact that surveillance powers are essentially only guided by the purpose pursued, oversight must ensure that the use of these powers adheres to the required procedure",[159] that is, that such structuring function as a corrective to the particular breadth and indeterminacy of the grounds justifying surveillance measures. Only in this way can the absence of the usual rule-of-law safeguards be compensated.[160]

---

[156] See Bundesamt für Sicherheit in der Informationstechnik, *Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess* (01.12.2022), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf.

[157] Comprehensively, Wischmeyer, *Informationssicherheitsrecht*, 2023, p 302-307.

[158] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 265 ff. (*BND – Ausland-Ausland-Fernmeldeaufklärung*) (umfassend zu den Anforderungen an Kontrollmechanismen); BVerfG, Order of 8 October 2024 - 1 BvR 1743/16, 1 BvR 2539/16, Rn. 171 (*BND-Cybergefahren*); BVerfG, Judgment of 20 April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Rn. 140 ff. (*BKA-Gesetz*)

[159] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 273 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[160] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 273 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

These grounds for the necessity of objective-law control mechanisms also apply in the case of vulnerability management: here, too, where existing vulnerabilities are kept secret there is no transparency, individual legal protection is normally not possible, and the parameters determining the decision — the conflicting aims of IT security and security-service intelligence — are essentially defined only in terms of their objectives.

This supports imposing high requirements on the scope and effectiveness of the control powers in this area too. In case of doubt, only a comprehensive, continuous objective legal review will do justice to this,[161] that is, the (possibility of) legal review of every decision to keep an IT vulnerability open.

It therefore seems conceivable that a two-part control should be established here as well: on the one hand, a court-like review by an independent adjudicatory body with a formalized procedure and effective case-by-case examination; on the other, an administrative legal review by an independent administrative body that can review individual decisions — on its own initiative, on a sample basis, or more comprehensively — as well as the underlying action processes, as the Bundesverfassungsgericht requires for certain decisions of the BND in the area of foreign intelligence.[162]

If such comprehensive control is not considered necessary, less intensive control regimes also come into consideration. For example, it is conceivable that the control body has only rights of objection, but no genuine rights of decision or intervention. Such limited control could be justified, for instance, on the ground that the legislature opts to design the official balancing and assessment process as a collegial decision[163] and that a certain reciprocal „control" is thereby already ensured through the first-instance decision-

---

[161] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 272 ff. (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[162] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 272-300 (*BND – Ausland-Ausland-Fernmeldeaufklärung*) (now implemented through the Unabhängiger Kontrollrat); Wischmeyer, *Informationssicherheitsrecht*, 2023, p 304.

[163] See infra B.V.1.

making process. Moreover, the exercise of the attack capabilities obtained via a vulnerability is, as a rule, once again subject to control.[164]

Irrespective of the question of the specific decision-making powers of the oversight infrastructure, it must meet certain constitutional minimum requirements:

It must be fully independent and equipped with sufficient resources and expertise — both technical and legal[165] — and must be able to access information that enables an appropriate assessment and review of the decisions. The latter means, in particular, that all decisions are to be sufficiently recorded and that the control body or bodies receive sufficient information for an effective exercise of their powers.[166]

Irrespective of possible limitations resulting from necessary measures of secrecy protection,[167] decisions on keeping IT vulnerabilities open must moreover be subject to parliamentary control. Thus they should in any event be brought within the oversight and assessment remit of the Parlamentarisches Kontrollgremium.[168]

---

[164] For example, through the control mechanisms of the *Unabhängiger Kontrollrat* or also through investigating judges in the criminal procedural area.

[165] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 285-288 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[166] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 288-295 (*BND – Ausland-Ausland-Fernmeldeaufklärung*); BVerfG, Judgment of 20 April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Rn. 141 (*BKA-Gesetz*).

[167] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 296 (*BND – Ausland-Ausland-Fernmeldeaufklärung*); see also Wischmeyer, *Informationssicherheit*, 2023, p 307.

[168] Regarding the inclusion or exclusion of the Parliamentary Control Committee in matters requiring confidentiality/secrecy control, BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 296-300 (*BND – Ausland-Ausland-Fernmeldeaufklärung*); See also Wischmeyer, *Informationssicherheit*, 2023, p 306.

8. Cybersecurity Measures to Protect State Knowledge of IT vulnerabilities

As already mentioned, the state's stockpiling of IT vulnerabilities also constitutes a considerable IT-security and fundamental-rights risk because official knowledge of vulnerabilities can be stolen by malicious actors.[169]

For this reason, it is a constitutional requirement[170] that particularly high information security standards, measured against the respective state of the art, apply to this storage.[171]

Generally applicable IT security requirements — for example under the BSIG, data-protection law, or the respectively applicable police and intelligence-service statutes[172] — will probably not be sufficient for this.

V. Design Recommendations Beyond Constitutional Requirements

Within the framework of constitutional necessities thus outlined, various concrete design options remain open to the legislature. This applies in particular as regards the design and selection of the decision-making body entrusted with vulnerability management (on this, 1.), the design of the

---

[169] Supra B.II.

[170] The Federal Constitutional Court has similarly imposed obligations on the legislature to ensure high IT security standards, for example, also with reference to the retention and transmission of telecommunications traffic data, BVerfG, Judgment of 2 March 2010 - 1 BvR 256/08, Rn. 221 ff. (*Vorratsdatenspeicherung*) bzw. BVerfG, Urteil vom 27. Mai 2020 - 1 BvR 1873/13, 1 BvR 2618/13, Rn. 188 (*Bestandsdatenauskunft II*) („An inseparable component of ordering a data storage obligation as well as the opening of private data holdings is, in addition to a normatively clear limitation of data use that meets the requirements, also the constitutionally mandated guarantee of data security.”).

[171] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, p 76; Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 33-34; Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 305-306.

[172] E.g. § 30 BSIG or Section 9 BKAG.

decision-making procedure (2.), and any transparency and reporting duties (on this, 3.).

1. Decision-Making Competence

The institutional design of the body leading the procedure and the procedural design of the decision-making procedure constitute central, but also particularly delicate, aspects of any vulnerability-management rules. Here, basic questions on the structure of the decision-making body are to be answered first, before some conceivable concrete designs are discussed.

a) Structure of the Decision-Making Body

By analogy with existing national governance systems — such as the *VEP*[173] or the United Kingdom's *Equities Process*[174] — and in agreement with existing proposals for a German design,[175] the decision on keeping a vulnerability open should not be taken within a single authority (neither the „discovering" security authority nor an „uninvolved" third authority[176]), but should be designed across authorities and departments as a stakeholder process. This makes it possible to ensure that the interests of all actors affected by the decision are taken into account and their respective expertise is brought in.

In organizational terms, this corresponds to a collegial body in which the bodies concerned can bring their positions into the coordination and decision-making process through representatives. At least the senior levels of the following should be involved: the Federal Ministries of the Interior; of

---

[173] *U.S. VEP* (2017) p 3-5.

[174] Government Communications Headquarters (GCHQ), *The Equities Process* (2018) https://www.gchq.gov.uk/information/equities-process.

[175] Wischmeyer, *Staatliche Nutzung von IT-Sicherheitslücken*, p 76 f.; Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 19 ff.; Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 300 ff.

[176] Regarding proposals to locate vulnerability management as a whole in a single authority, particularly in the BSI or the ZITiS, Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 300-302.

Defence; for Economic Affairs and Energy; of Justice and for Consumer Protection; and for Digital Affairs and State Modernization; as well as the BSI, ZITiS, the intelligence services (BfV, BND, and MAD), the police forces (BKA, BP), the Bundeswehr, and the Federal Office of Civil Protection and Disaster Assistance.

The decision-making procedure must be prepared, led, and supported. This requires an institutional embedding and framework that can take on such tasks (a „secretariat").[177] Since parts of the support work will require considerable IT-security-related knowledge (for example, to answer questions about the technical complexity of exploiting a discovered vulnerability or about the likelihood of patches), it must be ensured that such a secretariat can access corresponding expertise. This can be achieved through its own appropriately qualified staff or through the advisory involvement of other institutions, such as the BSI and ZITiS.

The secretariat must further meet the documentation and reporting tasks and should, ideally, also function as an institutional memory. In any event, it must be borne in mind that self-interests of the responsible institution can also assert themselves in the leadership, coordination, and support of the decision-making process; the choice of the responsible institution is therefore more than a merely technical question.

b) Possible Designs

Against this background, various institutions are conceivable as the secretariat of the procedure.

In favour of locating it at the BSI[178] is its comprehensive — in particular technical — expertise in matters of IT security. Against this, however, is the fact that the BSI, as a „defensive" authority, serves (only) the protection of IT

---

[177] Wischmeyer, *Informationssicherheit*, 2023, p 302.

[178] Proposed in *Koalitionsvertrag 2021-2025*, p 87, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

security according to its statutory mandate and acts politically as an advocate of the interests connected with it.[179] This could conflict with the neutral role of procedural leader. Moreover, the trust on which the BSI is necessarily dependent for performing its tasks in the IT security field should not be called into question by flanking or diluting this statutory mandate.[180] Ultimately, this is likely to speak against locating it at the BSI.

A location at ZITiS is to be assessed similarly. It appears incompatible — or at any rate difficult to reconcile — with ZITiS's orientation towards the development of offensive cyber capabilities.[181]

In favour of locating it at the Federal Chancellery is the fact that the Chancellery already performs coordination tasks between the individual departments and between the Federation and the Länder in numerous fields and represents „neutral" ground for embedding the decision-making process.[182] On the other hand, the Federal Chancellery (thus far) lacks relevant IT-security-related expertise. This could, however, be built up.

In favour of assigning responsibility to the National Cyber Defence Centre (NCAZ) is the fact that security authorities and the BSI already exchange views there today on matters of nationwide cyber security.[183] The absence of a statutory basis for the NCAZ, however, is a disadvantage. This could be created in the course of enacting a statutory vulnerability-management scheme.

---

[179] See also § 3 Abs. 1 Nr. 18 and Nr. 19 BSIG, according to which the BSI is only permitted to support security and other authorities insofar as this is necessary to prevent or investigate activities directed against IT security.

[180] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 20; Wischmeyer, *Informationssicherheit*, p 302; Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 301.

[181] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 301 f.

[182] Wischmeyer, *Informationssicherheit*, 2023, p 301 f.

[183] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 303 f.; the eight core members of the NCAZ are: MAD, BKA, BSI, BfV, BBK, BND, BPol and Bundeswehr-Kommando Cyber- und Informationsraum.

By contrast, the National Cyber Security Council (NCSR) appears rather less suitable, since no representatives of the security authorities currently take part in it and the involvement of business associations would make secrecy protection more difficult.

As an alternative to attaching it to an existing institution, the creation of a new body also comes into consideration.

2. Decision-Making Process

At least at the sub-statutory level, the process in which the decision on the secrecy or disclosure of the vulnerability is made should also be designed in more detail.

There can be little dispute about some of the procedural steps to be defined:

Authorities that obtain knowledge of a *zero-day* vulnerability must, if they wish to keep it open, report it to the secretariat within a short time (for example, one week). This report must contain a description and (initial) assessment of the vulnerability, providing at least information or assessments on the following aspects: the manner of obtaining, or the origin of, the knowledge of the vulnerability; the nature and severity of the vulnerability (description of the attack vector, degree of system access enabled, etc.);[184] the prevalence of the vulnerability or of the affected products, and the type of affected products or infrastructure; the extent to which knowledge of the vulnerability has spread and the likelihood of exploitation; the possibility and likelihood of patches (availability of maintainers, *end-of-life*, reachability of those affected, etc.); the possibility of

[184] E.g. assessed according to *Common Vulnerability Scoring System*, siehe FIRST.Org, Inc., *Common Vulnerability Scoring System Version 4.0: Specification Document (Version 1.2)* (2024).

mitigation measures; and the operational benefit („added value", dispensability of the vulnerability, etc.).[185]

The decision-making procedure must then leave all participating authorities sufficient time to analyse and assess the vulnerability, while at the same time keeping in view the timely reaching of a decision. An assessment period of one week and a meeting or decision cycle of one month, for example, appear appropriate.

If the decision is to disclose the vulnerability, this should be communicated to the BSI so that it can contact the affected vendor within the framework of its CVD process.[186]

If the decision is to withhold the vulnerability, the possibility and necessity of mitigation measures must, on the one hand, be discussed[187] and, on the other, the continued secure and secret safekeeping of the vulnerability must be ensured.[188] Precautions should be taken that, in the event of unexpected third-party knowledge, enable rapid disclosure of the vulnerability or other protective measures.[189] Moreover, a regular re-evaluation of the vulnerability — for example, annually or semi-annually — must take place.[190]

There is greater regulatory latitude with regard to the decision-making procedure. Conceivable in particular are consensus-oriented and vote-based decision-making procedures, whereby in the latter various decision quorums

---

[185] See also Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 23-30 and *U.S. VEP* (2017) p 13-14.

[186] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 305.

[187] See also oben B.IV.6.

[188] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 33 f.; see already supra B.IV.8.

[189] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 14.

[190] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 305; see also supra B.IV.8.

are possible.[191] Further, decision-making prerogatives (for example, for the „discovering" authority), veto rights, and staggered processes also come into consideration.[192]

Comparable to the VEP,[193] a consensus-oriented decision-making process appears preferable, in which consensus on the decision is sought and is ultimately also required in order to reach a decision.[194] Vote-based procedures carry the risk of arithmetical contingencies (for example, a numerically greater participation of security authorities), generate less political legitimacy, and can produce decision dynamics inappropriate to the matter at hand.

3. Transparency and Reporting Duties

Finally, statutory rules should also establish reporting duties to create transparency towards the public and, in particular, external experts, enabling a (rough) assessment and evaluation of the assessment procedure.[195] Such reports should contain at least information on the number of vulnerabilities that have become known and the proportions of disclosure, secrecy, and mitigation.

---

[191] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 23 advocates, for example, a blocking minority against the secrecy of vulnerabilities of approximately 15%..

[192] On the last point, see Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 23.

[193] *U.S. VEP* (2017) 7 f.

[194] In the U.S. VEP procedure, if there is no consensus in the committee regarding the option to be implemented, a vote is taken. This majority decision can then be challenged by a single participating authority. If such a challenge occurs, the decision is escalated to higher levels of the U.S. security architecture. At the end of these escalation paths stands the decision by the President, *U.S. VEP* (2017) 7 f.; in principle, such escalation procedures, for example also with the successive exclusion of certain previously involved actors, are also conceivable within the German framework.

[195] Herpig, *Schwachstellen-Management für mehr Sicherheit*, 2018, p 34.

VI. State Use of Third-Party Surveillance Capabilities

The discovery of vulnerabilities and *exploits* and the development of operational espionage tools require technical expertise that is often only very limitedly available at state institutions. For this reason too, drawing on external offensive cyber capabilities, including spyware tools, is today of considerable importance in the practice of the security authorities. This concerns both commercial vendors (so-called *commercial surveillance vendors*) and cooperation with foreign security and intelligence services. If only for reasons of practical relevance, the area of such service-based surveillance may therefore not be excluded from rules on vulnerability management. Moreover, this would also be doubtful in constitutional terms.[196] In the following, the drawing on commercial vendors (on this, 1.) and then the use of corresponding capabilities within the framework of state cooperation (on this, 2.) are examined more closely.

1. Commercial Surveillance Vendors

It can be assumed that at present the majority of German surveillance capabilities are based on knowledge or tools originating from commercial private spyware vendors.[197] In the following, this complex of service-based surveillance is briefly presented (on this, a.), before the specific risks of outsourced intrusion operations are then discussed (on this, b.) and classified within the existing constitutional case law and the remaining constitutional framework already presented (on this, c.). Finally, the requirements of constitutional law and of expediency regarding the regulation of service-based surveillance are set out (on this, d.).

---

[196] Infra B.VI.1.c).

[197] With this assessment for the U.S. context, Google Threat Analysis Group, *Buying Spying* (2024).

a) The Commercial Surveillance Industry: Structures and Practices

The demand for commercial surveillance tools has, over the past two decades, led to the emergence of a multibillion-euro but extremely opaque spyware market, which — through sometimes complex supply chains (so-called *exploitation supply chains*) — organizes the supply of such tools to state and private actors.[198] Actors on the supply side here are, in particular, private vulnerability researchers and *exploit* developers who discover vulnerabilities and develop software to exploit them; brokers who purchase and trade such capabilities; and *spyware-as-a-product* and *spyware-as-a-service* vendors that market complete, functioning surveillance solutions (from the so-called *delivery mechanism* to the tool for analysing the data spied out).[199]

State actors can make use of these offerings in various ways: on the one hand, they can purchase vulnerabilities and develop their own tools to exploit them. In that case, they acquire knowledge of a vulnerability and can — indeed must — run the vulnerability-management procedure with it. But they can also purchase *spying-as-a-service* or *spying-as-a-product* capabilities that enable them to infiltrate and spy out target devices without obtaining more detailed information about the exploited vulnerabilities or the design of the espionage software used.[200] In that case, they in principle obtain no knowledge of the exploited IT vulnerability on the disclosure of which a decision could be made. Comparable to this is the (probably significantly rarer) situation in which state actors do obtain relevant information about the exploited

---

[198] For a very good overview of this market and its characteristics and dynamics, see DeSombre Bernsen, *Crash (exploit) and burn* (2024) p 7-20; see also Roberts u.a., *Mythical Beasts and Where to Find Them* (2024).

[199] Categorization according to Google Threat Analysis Group, *Buying Spying* (2024) p 16-45.

[200] For an illustrative product offering of the spyware company Intellexa, including included services and prices, see Google Threat Analysis Group, *Buying Spying* (2024) p 30-33; Furthermore, subscription solutions are also offered in which state purchasers obtain access to, for example, all exploits that a company discovers within a certain period, see DeSombre Bernsen, *Crash (exploit) and burn* (2024) p 12.

vulnerability but, owing to a non-disclosure agreement, would not pass it on — that is, would either not even give it to other state bodies for review, or at any rate may not disclose the vulnerability to the vendor.

With regard to all products and services, it must be noted that the underlying supply chain can only rarely be fully clarified[201] and that state purchasers rarely obtain exclusive contracts — that is, the purchased product is, as a rule, simultaneously offered to other purchasers as well.

b) Risks of Using Commercial Spyware Services

The state's purchase of commercial surveillance tools entails dangers to IT security as well as to the liberty rights of individuals and to state interests — dangers that in part considerably exceed those triGrundgesetzered by state knowledge of vulnerabilities, but are at least comparable to them.

Where the state obtains surveillance capabilities from private parties, it is certain that (also) other actors — at any rate the selling company — know of the exploited vulnerability and can exploit it. This can also include authoritarian states that deploy surveillance capabilities in a targeted manner against the opposition and civil society, and even criminal actors such as ransomware operators.[202] Even where vendors state that they sell only to governments, or only to „Western" governments, such assurances can rarely be reliably verified. It must also be taken into account here that private vendors are economically acting actors oriented towards making profit, who

---

[201] Regarding the opacity of these supply chains and the widespread involvement of subcontractors, DeSombre Bernsen, *Crash (exploit) and burn* (2024) p 16-18.

[202] NSO Group, the company behind the spyware Pegasus, had, according to its own statements, in addition to its customers in 14 EU countries, also state purchasers in, among others, India, Saudi Arabia, the United Arab Emirates, Kazakhstan, Togo, Rwanda and Indonesia. The approximately 12,000 attacks annually targeted primarily politicians, opposition members, activists, scientists and journalists, see Meister, *Staatstrojaner Pegasus wird alle 40 Minuten eingesetzt* (22.06.2022) https://netzpolitik.org/2022/pega-untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/#2022-06-21_European-Parliament_PEGA_NSO.

must exceed high investment costs with even higher revenues.[203] Owing to the opacity and complexity of the market, it moreover often cannot be traced where the capabilities (vulnerabilities, *exploits*) on which an offered surveillance tool is based come from, and who else has knowledge of them.

Further, the protection of the deployed vulnerabilities against attackers cannot be controlled or verified either. The outsourcing of espionage activities therefore creates considerable counterintelligence risks.[204] It is known that private espionage vendors are regularly attacked by third parties, including state actors — among others, North Korea.[205] Such counterintelligence attacks can hardly come as a surprise, since the outsourced activities are among the most sensitive intelligence, military, and police operations of a state at all.[206]

In addition, there is always the danger that the commissioned companies misuse secret information transmitted to them for the identification of target persons,[207] or pass it on to other customers,[208] or even gain access to the extracted information.[209] In the proceedings between *WhatsApp* and the spyware vendor *NSO Group*, for example, employees of the espionage company testified that *NSO Group*'s customers transmit the target persons'

---

[203] Regarding the economic conditions under which such companies operate, see DeSombre Bernsen, *Crash (exploit) and burn* (2024) p 9-12.

[204] Deibert, *The Perils of Privatized Cyberwarfare* (2016) (with a list of known cases); see also supra B.II.

[205] DeSombre Bernsen, *Crash (exploit) and burn* (2024) p 10.

[206] Deibert, *The Perils of Privatized Cyberwarfare* (2016).

[207] Spyware companies regularly do not make clear statements about how much insight they have into the operations carried out through their systems, Deibert, *The Perils of Privatized Cyberwarfare* (2016).

[208] Deibert, *The Perils of Privatized Cyberwarfare* (2016).

[209] European Parliament, *Recommendation*, p 10.

telephone numbers and that the company controls the infiltration and extraction process.[210]

Overall, transparency and possibilities of public control are weakened by the outsourcing to the private sector, which in this area places quite particular emphasis on secrecy and opacity.[211]

Structurally, state demand for private surveillance tools moreover feeds a corrupt ecosystem of commercial *threat actors* that attack the security of the most fundamental IT infrastructure globally and universally undermine IT security.[212] Even „no-buy" lists or state sanctions against particularly aggressive actors[213] can do little to change this, especially since sanctioned firms attempt to remain in business undetected via shell companies.[214]

---

[210] However, it remains unclear whether NSO Group also had access to the extracted information; Smally, *Testimony from NSO Group raises questions about its culpability for spyware abuses* (19.11.2024) https://therecord.media/nso-group-whatsapp-case-documents.

[211] The Citizen Lab, *Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the United Nations Working Group on the Use of Mercenaries* (2026) p 3.

[212] Google Threat Analysis Group, *Buying Spying* (2024) p 5; Deibert, *The Perils of Privatized Cyberwarfare* (2016) „Outsourcing these operations to the private sector will incentivize a race to discover, acquire, and, crucially, hoard software vulnerabilities not just in modern phones but also in critical infrastructure, ... This arms race will inevitably lead firms to dig deeper into the increasingly invasive internet of things and operational technology infrastructure upon which modern society relies, such as consumer security cameras or Siemens industrial controllers, found throughout sensitive systems, including electrical grids and water treatment plants. The service of one actor's narrow national security interests will spawn an ever-growing collective insecurity for the rest of the globe, at the deepest level of infrastructure on which all of society critically depends"; European Parliament, *Recommendation*, p 5.

[213] See e.g. U.S. Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (03.11.2021) abrufbar unter https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[214] Deibert, *The Perils of Privatized Cyberwarfare* (2016); In 2023, the FBI announced that it had discovered that a supplier had acted as a front company for the NSO Group sanctioned by the United States, see Krempl, *Trotz Verbot: FBI hat über Vertragsfirma NSO-Spyware finanziert* (31.07.2023) https://www.heise.de/news/Trotz-Verbot-FBI-hat-ueber-

Finally, the purchase of private surveillance tools legitimizes the corresponding markets for IT insecurity and contributes to the loss of one's own reputation and credibility and to the erosion of international cyber norms — factors that, in the long term, fuel both the decline of the global IT security level and the proliferation of illegitimate surveillance capabilities.[215]

c) Constitutional Assessment

The BVerfG's decision on IT vulnerabilities expressly limits the existence of a duty to regulate to those cases in which state authorities themselves have knowledge of a specific vulnerability, regardless of how they obtained that knowledge.[216]

On closer constitutional analysis, however, it is clear that the outsourcing of attack capabilities to private actors — in other words, the exploitation of privately stockpiled vulnerabilities — cannot be exempted from this duty to regulate either.

This can ultimately be derived already from the fact that the aims and effectiveness of state vulnerability management could be wholly undermined if the state could draw on private infiltration capabilities without restriction, so long as it merely obtained no knowledge of the vulnerabilities used in doing so.[217] Indeed, such a legal situation would give security authorities strong incentives to resort to private infiltration capabilities and thereby promote a shift to structurally even more dangerous knowledge of vulnerabilities, or the circumvention of the vulnerability-assessment procedure.

Vertragsfirma-NSO-Spyware-finanziert-9231066.html; see also European Parliament, *Recommendation*, 7-8.

[215] Deibert, *The Perils of Privatized Cyberwarfare* (2016) talking about an “arms race“; The Citizen Lab, *Submission*, p 5-6.

[216] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 40 (*IT-Sicherheitslücken*).

[217] Deibert, *The Perils of Privatized Cyberwarfare* (2016) „However, it is difficult to see how any internal government VEP can remain effective when the responsibility to discover and stockpile [exploits] to private contractors, effectively placing the inventory and decision-making outside the scope of formal oversight procedures.”.

An analysis of the specifically constitutional-court reasoning likewise makes clear that the involvement of private espionage capabilities cannot be exempted from the assessment duty. For the Constitutional Court bases this duty precisely on the general „Pflicht, dazu beizutragen, dass die Integrität und Vertraulichkeit informationstechnischer Systeme gegen Angriffe durch Dritte geschützt"[218] wird, which is grounded in the high potential for endangerment and harm posed by vulnerabilities and the absence of any possibility of self-protection.[219] Moreover, in the cases of drawing on private espionage capabilities, too, there is a specific responsibility on the part of the state which — even if it may not itself be able to initiate the remedying of the vulnerability — as a (potential) purchaser makes its continued keeping-open necessary.

The transferability of the positive-obligations argument is further supported by the constitutional-court requirements on the structurally comparable cooperation with foreign intelligence services. In its judgment on foreign–foreign signals intelligence, the Bundesverfassungsgericht made clear that, while the Grundgesetz does not in principle preclude cooperation with other intelligence services, rules allowing cooperation with foreign intelligence services satisfy fundamental-rights requirements only if they ensure that the rule-of-law limits are not circumvented through the mutual exchange and that the Federal Intelligence Service's responsibility for the data it collects and analyses remains preserved at its core.[220]

---

[218] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 40 (*IT-Sicherheitslücken*).

[219] BVerfG, Order of 8 June 2021 - 1 BvR 2771/18, Rn. 34-39 (*IT-Sicherheitslücken*).

[220] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Ls. 7, Rn. 244 ff. (*BND – Ausland-Ausland-Fernmeldeaufklärung*).; the corresponding regulations are contained in §§ 13-17 BNDG; see also BVerfG, Judgment of 20 April 2016 - 1 BvR 966/09, 1 BvR 1140/09, Rn. 327 (*BKA-Gesetz*) „The limits of domestic data collection and processing under the Basic Law must not be undermined in their substance through an exchange between security authorities. The legislature must therefore ensure that this fundamental rights protection is not weakened either by the transmission of data collected by German authorities to foreign countries and international organizations, nor by the receipt and use of data obtained by foreign authorities in violation of human rights".

In particular, fundamental-rights standards — such as collection prohibitions — may not be circumvented by accepting information from other security services by way of a „multilateral exchange".[221]

The surveillance capabilities of other services may therefore be accessed, and the data they collect obtained and used, only where corresponding statutory bases exist[222] that take account of the „possibility inherent in such practices that obligations under domestic law could be circumvented [...] and the specific risks to fundamental rights which may arise from cooperation".[223]

Specifically, prior to such cooperation it would, for example, have to be ascertained that data-protection standards and rule-of-law principles would be observed by the partner service, and such assurances would have to be underpinned by „substantial assurances" of the partner services.[224] A „preventive court-like assessment" could also be required.[225]

Constitutionally required control mechanisms may not be impeded by invoking the so-called *Third Party Rule*, according to which information from foreign security services may not be passed on to third parties without their consent.[226] The legislature would therefore have to ensure that the security services, in their arrangements with partners, in any event obtain the corresponding authorizations, so that they may pass on all information

---

[221] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 248-249 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[222] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 250 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[223] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 250 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[224] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 233-243 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[225] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 240 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[226] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 291 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

relevant to control to the corresponding control bodies, or that such bodies are not classified as a *third party*.[227]

Even though these are different regulatory questions: if the Constitution imposes such fine-grained regulatory requirements even on surveillance cooperation with („allied") state actors, it seems out of the question that the outsourcing of surveillance activities to private actors — and thus to actors not bound by fundamental and human rights — should escape any constitutional containment.

d) Constitutional Requirements and Appropriate Design

If, then, the drawing on private surveillance capabilities cannot be wholly exempted from the duty of vulnerability management[228] or left unregulated, this does not yet clarify how exactly such processes must be contained, or which regulatory options are available to the legislature here. Conceivable, among others, are the following regulatory models:

In view of the high IT-security and fundamental-rights risks entailed by resorting to private espionage companies,[229] it is conceivable, first, to prohibit such cooperation in principle. The state would then be dependent on developing its own intelligence capabilities or on obtaining them from partner services. In the long term, this would also end the dependence — viewed extremely critically even in security circles — on privately developed and thus structurally insecure and uncontrollable espionage tools.

A rule under which the state may indeed purchase private surveillance tools but must also feed them into vulnerability management and, where applicable, must disclose the vulnerability to the vendor would be similarly prohibitive. Effectively, this would mean that the state must acquire an

---

[227] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 294-295 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[228] However, this is essentially the case within the framework of *U.S. VEP* (2017) p 9-10.

[229] See B.VI.1.b).

exclusive licence to the developed product. Vendors will agree to this only at correspondingly high prices.

Further, an assessment model comparable to the requirements established by the Constitutional Court for cooperation with foreign intelligence services would come into consideration.[230] Before cooperating with private spyware vendors, the state would then have to examine certain standards of legality and the rule of law in a due-diligence procedure. Comparable to the requirements that exist for cooperation with intelligence services, the state could, for instance, be obliged to ascertain that certain data-protection guarantees — in particular those of data security — as well as rule-of-law principles are observed.[231] The latter could consist, for example, in affected vendors demonstrably not selling their products to authoritarian governments or „rogue states" and offering sufficient assurance that these do not reach such actors by other routes either; that the products are not deployed against protected groups of persons; and that no (unreasonable) counterintelligence risks emanate from the vendors.[232] The assessment must not, of course, be subject to the free discretion of the assessing state institutions and would have to be based on „substantive, reality-based and up-to-date information".[233] It would have to be reinforced by rights to

---

[230] See supra B.IV.7; see also European Parliament, *Recommendation*, p 22 „companies applying in a public procurement process to be suppliers should undergo a vetting process which includes the company's response to human rights violations committed with their software and whether the technology relies on data gathered in undemocratic and abusive surveillance practices".

[231] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 231-237 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[232] Manageable standards and definitions for these principles could also be adopted from Executive Order 14093 of former U.S. President Joe Biden, Executive Office of the President, *Executive Order 14093 - Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security* (27.03.2023).

[233] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 241 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

information[234] and effective sanction mechanisms against the spyware vendors. In particular, vendors should be obliged, by way of a „Know Your Vendor" procedure, to disclose suppliers and investors.[235] Further, the assessment would necessarily have to be documented and thereby made accessible to independent control.

Procedurally, such an assessment procedure, too, could be organized in the sense of a „Spyware Equities Process" similar to the procedure proposed for the assessment of vulnerabilities.[236] The recruiting or approached authority would then, in a preliminary examination, have to obtain the necessary information in order to carry out an initial assessment under the applicable substantive standards, which would then be submitted to the body for decision. It is then also important that the monitoring of the vendors be continuously maintained.

In any event, the partner company's compliance with legal requirements should be secured by contractual arrangements, even though these of course provide no guarantee of actual compliance. Such arrangements could also contain a duty that the tool must, as far as possible, be designed and/or configured such that, even technically, only what can also be legally permitted is possible („rule-of-law-by-design").[237] A duty to use traceability markers is also conceivable, which leave on infiltrated devices a signature or similar technical artefact by which it can subsequently be verified who

---

[234] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 237 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[235] Roberts u.a., *Mythical Beasts and Where to Find Them* (2024) p 23; such obligations are particularly necessary to prevent the circumvention of effective controls through front companies and other obfuscation tactics; see also Panagiotopoulos, *Policymakers Ignore Spyware Middlemen Driving Global Proliferation* (18.03.2026).

[236] The European Parliament is also of the opinion that the purchase of spyware must be able to be reviewed by an independent control authority, European Parliament, *Recommendation*, p 22 „Concludes that when a Member State has purchased spyware, the acquisition must be auditable by an independent, impartial audit body with appropriate clearance".

[237] See also European Parliament, *Recommendation*, p 21-22.

initiated the deployment of the spyware and when.[238] In any event, contracts with spyware vendors must ensure that purchasing authorities are not prevented from informing other state bodies about vulnerabilities of the affected infrastructure; only in this way can it be ensured that the state can at least take effective self-protection measures.

Flanking rules — for instance, a court-like prior review or the condition that private espionage software may be resorted to only where this is absolutely necessary for the performance of statutory tasks — should further secure the deployment. A duty on the part of the company to disclose the exploited vulnerabilities is also conceivable.

Alternatively, such standards could also be enforced in a certification model, in which vendors, before they can offer the state spyware products, must first obtain a corresponding certification, which is then subjected to regular auditing (so-called *white listing*). This would have the particular advantage that resources would be pooled in the evaluation and a visible market incentive for „clean" vendors would be created. Harsh sanctions against companies that violate contractual arrangements or statutory law could counteract the currently prevailing culture of impunity and lack of accountability.[239]

Beyond this, it also seems conceivable to prohibit entirely the drawing on „hacking-as-a-service" services — in which, unlike the purchase of espionage tools, infiltration and extraction are controlled and carried out by the third-party company — since the offering companies regularly obtain even more

---

[238] European Parliament, *Recommendation*, p 21 „a marker needs to be included in the surveillance software so that oversight bodies can unambiguously identify the deployer in the event of suspicion of abuse; the mandatory signature for each spyware deployment should consist of an individual label for the acting authority, the type of spyware used and an anonymised case number".

[239] The Citizen Lab, *Submission*, p 6-7.

extensive access to sensitive information in these cases, or since such access can at any rate be prevented even less easily.[240]

A vendor-side enforcement of substantive requirements in the form of direct market regulation — for example, such that, under a „rule-of-law-by-design" approach, only such technologies may be sold as offer sufficient assurance of compliance with an appropriate level of protection (e.g. through software design, encryption, authentication mechanisms) — also comes into consideration, but is, if at all, best pursued at the Union level.[241]

2. Cooperation with Foreign Security Authorities

It can be assumed that foreign partner services, too, regularly make offensive cyber capabilities available to German security authorities. As also applies to resorting to commercially offered surveillance capabilities,[242] the aim and effectiveness of rules on vulnerability management may not be undermined by such cooperation either. In regulatory terms, a transfer of the examination duties that the Bundesverfassungsgericht established for the area of intelligence cooperation in signals intelligence suggests itself.[243] How these requirements can be transferred to the review of offensive cyber capabilities has already been explained here in the context of drawing on commercial offerings.[244]

---

[240] European Parliament, *Recommendation*, p 22.

[241] This is also proposed by the EU Parliament, which points out in this respect that citizens in third countries enjoy better protection under the EU's Dual-Use Regulation than EU residents, European Parliament, *Recommendation*, p 21-22.

[242] Supra B.VI.1.

[243] BVerfG, Judgment of 19 May 2020 - 1 BvR 2835/17, Rn. 233-242 (*BND – Ausland-Ausland-Fernmeldeaufklärung*).

[244] Supra B.VI.1.d).

C. The Framework of Legislative Competence

Having worked out in Part B. that the German state is under a fundamental-rights obligation to regulate vulnerability management and the purchase of spyware, the question now arises whether, and to what extent, it — and in particular the federal legislature — is also competent to do so.

In other words, it must be clarified which institutional level is at all competent, in terms of legislative competence, to enact such statutory rules. In this respect, the European Union comes into consideration, and at the national level the federal legislature and the Länder. In the following, it is therefore first examined whether the European Union is competent to regulate the matters affected here (I.), before, in a second step, it is examined who, within the intra-German competence structure, has the regulatory competence (III.). Since the regulatory discretion of national legislatures could, owing to the primacy of EU law, also be limited by secondary EU law, it must further be examined whether EU law already today imposes requirements on national vulnerability management (II.).

The existence of a competence depends decisively on the exact contours and content of the planned regulation. The following remarks are therefore based on the desire for a substantive regulation — as comprehensive as possible and covering as many state institutions as possible — of the duty to implement a vulnerability-management procedure, as well as for a regulation of the state's handling of commercial spyware tools.

I. Competence of the European Union

It first comes into consideration that the European Union has the competence to regulate the matters mentioned.

1. Legal bases

Under the principle of conferral, the European Union may act only insofar as a corresponding competence has been conferred on it in the Treaties (TEU and TFEU).

Various competence bases come into consideration in this respect.

a) Art. 114(1) sentence 2 TFEU

Under Art. 114(1) sentence 2 TFEU, the EU may adopt measures for the approximation of the Member States' legal and administrative provisions which have as their object the establishment and functioning of the internal market. On the basis of this competence, the EU is thus permitted to remove obstacles to European economic activity in order to contribute to the realization of a European internal market.[245] Even though Art. 114 TFEU does not establish a general regulatory competence, it does enable approximation measures in a large number of legal fields[246] and is interpreted extensively by the European legislatures, largely without objection on the part of the CJEU.[247] In the field of information security law, the Union legislature assumes that measures for the general raising of cybersecurity, for the defence against cyberattacks, and also for strengthening „trust in the digital single market" can be covered by Art. 114 TFEU.[248] Thus Art. 114 TFEU also supports, for example, the establishment of the European Union Agency for Network and Information Security, ENISA,[249] as well as the detailed norms of the NIS 2 Directive and the Cybersecurity Act (CSA), which assign the agency, on a broad scale, even highly abstract, „market-distant" competences — for

---

[245] Calliess/Ruffert/*Korte* (2022) Art. 114 TFEU Rn. 2, 40.

[246] Grabitz/Hilf/Nettesheim/*Tietje* (September 2025) Art. 114 TFEU Rn. 77-79.

[247] Streinz/*Schröder* (2018) Art. 114 TFEU Rn. 33.

[248] See e.g. Rec 2, 7 Cybersecurity Act.

[249] CJEU, Judgment of 2 May 2006, C-217/04, Rn. 48 ff. (ENISA).

instance, to advise the Member States in the field of cybersecurity research.[250]

Against this background, it is anything but far-fetched that the Union legislature also sees statutory rules on the state's handling of IT vulnerabilities as covered by Art. 114(1) sentence 2 TFEU, since the holding of such vulnerabilities has effects on the functioning of the digital internal market.[251] The position is similar with rules on the purchase of commercial spyware capabilities.[252] Such rules, moreover, technically have an even stronger market finality. In both cases, however, it would then have to be examined, in the light of the specific regulatory proposal, to what extent uniform rules to remove trade barriers in this area are actually necessary, or whether this would actually be the object pursued by such rules. This appears conceivable — in particular for rules on the purchase of spyware capabilities — but also depends on whether it can be proven that, owing to differing national rules, trade barriers or distortions of competition actually exist and that the measure is, in essence, aimed at overcoming them.[253]

b) Art. 16(2) subpara. 1 sentence 2 TFEU

The competence under Art. 16(2) subpara. 1 sentence 2 TFEU, which concerns the protection of personal data, is by contrast unlikely to be

---

[250] See also Wischmeyer, *Informationssicherheit*, 2023, p 164 ff. see also Calliess/Baumgarten, Cybersecurity in the EU, German L. J. 21 (2020), p 1149 (1164).

[251] Disagreeing Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 278.

[252] The European Parliament appears to assume that there is EU competence in this respect, European Parliament, *Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation)* (P9_TA(2023)0244), p 18 „the configuration of spyware that is imported into the EU and otherwise placed on the market should be regulated by way of a measure based on Article 114 TFEU"; the Parliament also proposes, furthermore, to regulate the offering and sale of spyware directly on the market side; an EU competence seems likely for such a regulation, European Parliament, *Recommendation*, p 21-22 „Emphasises that only spyware that is designed so that it enables and facilitates the functionality of spyware according to the legislative framework as set out in paragraph 32 may be placed on the internal market, developed or used in the Union".

[253] See also regarding the standards established by the CJEU Streinz/*Schröder* (2018) Art. 114 TFEU Rn. 19-33, with some instructive, albeit not very coherent examples.

applicable.[254] For even though the CJEU usually views incursions — mediated via Art. 16(2) subpara. 1 sentence 2 TFEU — into regulatory competences reserved to the Member States indulgently,[255] neither decisions on keeping a vulnerability open nor decisions on the purchase of spyware can, in essence, be understood as rules on the „processing of personal data".[256]

c) Judicial and Police Cooperation

Further competence bases come into consideration in Chapters 4 („Judicial cooperation in criminal matters") and 5 („Police cooperation") of Title V of the TFEU („Area of Freedom, Security and Justice").[257]

Specifically, under Art. 82(1) subpara. 2 point (d) TFEU, the EU may, in the area of criminal prosecution, adopt measures to „facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions", whereby these may not lead to a „harmonisation of the legal rules of the Member States".[258] Under paragraph 2 subpara. 2, by contrast, even such approximation in the form of minimum rules is permissible where it concerns the area of the „mutual admissibility of evidence between Member States" (point (a)) or „any other specific aspects of criminal procedure which the Council has identified in advance by a

---

[254] See also *Buntrock, Staatlicher Umgang mit IT-Sicherheitslücken, 2025*, p 278.

[255] See e.g. CJEU, Judgment of 30 March 2023, C-34/21, Rn. 32 ff. (*Hauptpersonalrat*) (regarding the regulation of online education despite the member states' competence to shape the education system).

[256] Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 278; the EU Parliament also does not base any of its regulatory proposals on Art. 16 TFEU, European Parliament, *Recommendation*.

[257] The EU Parliament also appears to assume this without conducting a more detailed analysis of the conceivable competence titles, European Parliament, *Recommendation*, p 18.

[258] Streinz/*Satzger* (2018) Art. 82 TFEU Rn. 16 ff.

decision" (point (d)). Admittedly, the European legislature (dubiously) assumes that not only measures establishing certain standards of cooperation — such as standardized data formats — can be based on these provisions.[259] More than minimum standards for the cross-border admissibility of evidence obtained with the help of vulnerabilities or spyware,[260] however, will not be achievable via Art. 82 TFEU.

Under Art. 87(2) point (a) TFEU, the EU may, in the area of police cooperation, adopt measures concerning the „collection, storage, processing, analysis and exchange of relevant information". However, neither standards on the disclosure or secrecy of vulnerabilities nor standards on the use of commercial spyware capabilities can be regarded as aspects of such „informational cooperation" between police authorities.[261] Under Art. 87(2) point (c) TFEU, the EU may indeed also regulate „common investigative techniques", but these may concern only the „detection of serious forms of organised crime". Finally, where there is unanimity in the Council, measures concerning the „operational cooperation" of police authorities may also be adopted under Art. 87(3) TFEU. This probably covers „"any joint coordination or alignment with respect to police or judicial measures in the field of police prevention of danger and police criminal prosecution ",[262] but also leaves considerable room for interpretation in detail. In this provision, too, however,

---

[259] The PNR Directive, which requires member states to oblige airlines to retain certain passenger data, was also based on Article 82(1)(d) TFEU.

[260] In particular, uniform minimum requirements under which evidence obtained through a security vulnerability or spyware in one member state is admissible in another member state (for example, documentation, integrity or chain of custody requirements).

[261] Similarly Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 279; classic examples of this are, for instance, the search systems of the Schengen Information System or the Visa Information System.

[262] Calliess/Ruffert/*Suhr* (2022) Art. 87 TFEU Rn. 24.

one cannot see a general competence for the regulation of requirements on vulnerability management and spyware purchase.[263]

d) Result

In the result, it thus comes into consideration that Union rules on vulnerability management, as well as on the purchase of commercially marketed spyware, can be based on Art. 114(1) sentence 2 TFEU. On Art. 82 TFEU, at most minimum standards on the usability, in criminal prosecution, of evidence obtained through such attack routes could be based, but not actual rules on vulnerability management. These are in each case shared competences under Art. 4 TFEU, so that, under Art. 2(2) TFEU, the Member States may act in a regulatory capacity „to the extent that the Union has not exercised its competence".

2. Limitations on Competences

However, even the competences expressly conferred on the Union are subject to certain reservations or limitations.

Of particular relevance to the present considerations is Art. 4(2) sentence 2 TEU, according to which the Union must respect Member States' „essential State functions, including [...] safeguarding national security". Accordingly, under Art. 4(2) sentence 3 TEU, „national security remains the sole responsibility of each Member State ".

Accordingly, existing Union rules in the field of IT security, too, contain exceptions for the area of „national security", in part also of „public security".[264] The EU Parliament, too, concedes that the use of spyware for

---

[263] Disagreeing Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 280.

[264] See, for example, Article 1(2) Cybersecurity Act "This Regulation does not affect the competences of the member states for activities relating to public security, defence, national security and State action in the criminal law sphere."; Article 2(7) NIS-2 Directive "This Directive does not apply to public administration bodies exercising activities in the fields of national security, public security, defence or Law Enforcement, including the prevention, investigation, detection and prosecution of criminal offences."; Article 1(5) Cyber Solidarity Act "This Regulation does not affect the fundamental State functions of the

national-security concerns may, at most, be „indirectly" regulated at Union level.[265]

What is to be regarded as a regulation of „national security", however, has not yet been conclusively clarified.[266] In principle, the concept is understood more narrowly than those of „public" or „internal security".[267] It is also clear that the CJEU has, in the past, tended to interpret corresponding sectoral exceptions narrowly, and has regarded even national measures that clearly concern the activities of the intelligence services as covered by EU law.[268] In the words of the CJEU, moreover, „the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law".[269]

Nonetheless, there is much to suggests that Union rules which regulate *specifically and directly* the state's handling of IT vulnerabilities or commercial spyware by intelligence services — potentially also by police authorities — are to be regarded as rules in the area of „national security" and

---

member states, including safeguarding territorial integrity, maintaining public order and protecting national security. In particular, national security remains solely the responsibility of each member state.".

[265] European Parliament, *Recommendation*, p 18 „notes that the use of spyware for national security purposes may only be indirectly regulated through, for example, fundamental rights and rules relating to data protection".

[266] European Parliament, *Recommendation*, p 23; see also *Tzanou*/*Vogiatzoglou*, European Papers eJournal (18.11.2025); Sandhu, *Squaring the Circle: The CJEU between Fundamental Rights Guardian and Architect of a Security Union*, Verfassungsblog, 2024.12.02.

[267] See also European Parliament, *Recommendation*, p 23; Article 15 of Directive 2002/58 equates "national security" with "security of the state".

[268] Siehe etwa CJEU, Judgment of 21 December 2016, C-203/15 and C-698/15, Rn. 75 ff. (*Tele2 Sverige*); CJEU, Judgment of 2 October 2018, C-207/16, Rn. 29 ff. (*Ministerio Fiscal*); CJEU, Judgment of 6 October 2020, C-623/17, Rn. 44 ff. (*Privacy International*); CJEU, Judgment of 6 October 2020, C-511/18 et al, Rn. 99 ff. (*La Quadrature du Net*).

[269] CJEU, Judgment of 6 October 2020, C-511/18 et al, Rn. 99 ff. (*La Quadrature du Net*) (with further references).

would thus be contrary to the allocation of competences. This is supported, on the one hand, by the fact that the judgments mentioned each concerned only (negatively) the sectoral exception or competence assignment for national-security measures in Art. 15 ePrivacy Directive — and thus the reach of EU law — but not (positively) the Union's legislative competences. And, on the other hand, by the fact that the legal act concerned, the ePrivacy Directive, undoubtedly covers many rules that clearly cannot be assigned to the area of national security.

In addition, Art. 346(1) point (a) TFEU could also stand in the way of a Union obligation to conduct vulnerability management, or of its enforcement without exception.[270] This provides that a Member State „nicht verpflichtet [ist], Auskünfte zu erteilen, deren Preisgabe seines Erachtens seinen wesentlichen Sicherheitsinteressen widerspricht".[271] Even though the CJEU affirms in settled case law that Art. 346 TFEU does not „contain[...] an inherent general exception excluding all measures taken for reasons of public security from the scope of European Union law ",[272] and that the provision is furthermore to be interpreted narrowly,[273] the norm does explicitly grant the Member States a margin of discretion,[274] which the Court appears to treat rather circumspectly.[275]

3. Result

In the result, regulation of vulnerability and spyware management by the EU therefore comes into consideration only to a limited extent. The EU could

---

[270] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 280 f.

[271] According to prevailing opinion in the literature, the provision also covers "disclosures" to individuals and the public, Calliess/Ruffert/*Wegener* (2022) Art. 346 TFEU Rn. 5 (with further references).

[272] See only CJEU, Judgment of 4 March 2010, C-38/06, Rn. 62 (*Commission/Portugal*).

[273] See only CJEU, Judgment of 20 March 2018, C-187/16, Rn. 77 (*Commission/Austria*).

[274] Calliess/Ruffert/*Wegener* (2022), Art. 346 TFEU Rn. 3.

[275] Calliess/Ruffert/*Wegener* (2022), Art. 346 TFEU Rn. 3.

probably, on the basis of Art. 114(1) sentence 2 TFEU, impose vendor-side requirements on the sale of spyware software within EU territory. The introduction of a duty of state vulnerability management by security authorities, by contrast, appears precluded by the competence limit of „national security“ under Art. 4(2) sentence 3 TEU.

II. Requirements under Existing EU Law

Even if the Union should have no competence to enact statutory rules on the state's handling of IT vulnerabilities or spyware,[276] it does come into consideration that it may regulate — or has already regulated — certain partial aspects of these fields of action.[277] Also because rules at the national level may not, owing to the primacy of EU law, violate Union requirements, the following must therefore examine whether existing rules of EU law already today regulate certain sub-areas of vulnerability management or of the purchase of spyware.

1. NIS 2 Directive

The NIS 2 Directive constitutes the currently central legal act of Union IT-security legislation. It obliges, in particular, operators of critical infrastructure and other so-called „essential and important entities” to take cyber-risk-management measures and to report security incidents.[278] Under Art. 21(2) point (e) NIS 2 Directive, this also covers measures on the „ vulnerability handling and disclosure”.

„Public administration entities”, too, are regarded as „essential entities” under Art. 3(1) point (d) and Art. 2(2) point (f)(i) NIS 2 Directive and must

---

[276] Supra C.I.

[277] See also Geiger/Khan/Kotzur/Kirchmair/*Geiger/Kirchmair* (2023) Art. 5 TEU Rn. 3; too narrow Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 281, who argues that the effects of existing Union legal acts on vulnerability management are in any case contrary to Union law.

[278] Art. 20 ff. NIS-2-RL.

accordingly fulfil the IT-security obligations provided for. Under Art. 2(6), however, the Directive provides that it „is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order". Under Art. 2(7), the Directive therefore expressly does not apply to „public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences". To this end, the Member States may therefore, under Art. 2(8) NIS 2 Directive, exempt such authorities — and also entities that provide services exclusively for such authorities — from the substantive IT-security obligations. The German legislature made use of this exemption option through the NIS2UmsCG in § 37(2) and (3) BSIG.[279]

Further, under Art. 2(11), the Directive does not cover „the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence", and Art. 346 TFEU remains unaffected under Art. 2(13) NIS 2 Directive.[280]

Finally, it must be borne in mind that the NIS 2 Directive obliges only to measures „to manage the risks posed to the security of network and information systems *which those entities use for their operations or for the provision of their services*, and to prevent or minimise the impact of incidents on recipients of their services and on other services". Accordingly, the discovery of a vulnerability can, in any event, oblige to measures (such as reporting the vulnerability) only where the vulnerability affects network or

---

[279] According to this, the Federal Ministry of the Interior is responsible for this decision. It can order an exemption on the proposal of the Federal Chancellery and various ministries or on its own initiative. The affected institutions do not have a right to apply.

[280] Supra C.I.2.

information systems that the authority itself uses for its operation,[281] or where the discovery can be understood as a „security incident", that is, as an „event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems". Both are conceivable but appear, for the standard case, rather unlikely.[282]

In particular against the background of the possibility of exempting the relevant (security) authorities, the NIS 2 Directive will therefore have no relevant influence on the questions of vulnerability management and spyware purchase affected here.

2. ePrivacy Directive

The ePrivacy Directive serves to protect privacy in electronic communications. Under Art. 5 ePrivacy Directive, the Member States for this purpose „shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation". They must in particular prohibit „listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned", Art. 5(1) sentence 2 ePrivacy Directive.

However, under Art. 5(1) sentence 2 in fine in conjunction with Art. 15, national exception rules are permissible, provided that these are „necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and

---

[281] This can of course raise difficult interpretive questions about what is to be understood as operation and service of a particular authority.

[282] Too broadly rejecting Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 283.

the prevention, investigation, detection and prosecution of criminal offences".

On the basis of Art. 5 ePrivacy Directive, the CJEU in 2020 and 2022 declared the national data-retention rules of France, the United Kingdom, and Germany contrary to EU law,[283] but then, in 2024, declared France's new data-retention rules permissible.[284]

Whether the ePrivacy Directive has any influence on national requirements on vulnerability management or spyware purchase depends on whether such practices concern or impair „ confidentiality of communications and the related traffic data by means of a public communications network". It is, first, beyond doubt that state-used vulnerabilities can in fact impair the confidentiality of messages transmitted via communications services covered by the ePrivacy Directive (e.g. messenger services). Against the coverage of the rules in question under Art. 5 ePrivacy Directive, however, is the fact that the examples mentioned there („listening, tapping, storage or other kinds of interception") have in view the actual interception of messages rather than the possession of infrastructure that can potentially be used for interception (e.g. IT vulnerabilities, spyware). This corresponds to the fact that the rules seek to protect the confidentiality of *messages*, but not of *communications services*.

Nonetheless, it is not inconceivable that, by way of an extensive interpretation, knowledge of vulnerabilities or purchased spyware, too, could be understood as an impairment — covered by Art. 5 ePrivacy Directive — of the confidentiality of transmitted messages, which could consequently be introduced nationally only in compliance with the fundamental-rights guarantees provided for in Art. 5(1) sentence 2 in fine in conjunction with

---

[283] CJEU, Judgment of 6 October 2020, C-511/18 (*La Quadrature du Net ua*); CJEU, Judgment of 6 October 2020, C-623/17 (*Privacy International*); CJEU, Judgment of 20 September 2022, C-793/19 und C-794/19 (*SpaceNet*).

[284] CJEU, Judgment of 30 April 2024, C-470/21 (*La Quadrature du Net*).

Art. 15 ePrivacy Directive.[285] Specific requirements on the design of vulnerability management do not, however, follow from the provision.

3. GDPR

The GDPR constitutes the central cross-sectoral data-protection law of the EU, imposing data-protection requirements on private and public bodies alike.

However, it applies only where the processing of „personal data" is concerned. This is not the case with the decision on keeping open or reporting a vulnerability itself,[286] so that provisions on vulnerability management fall outside the regulatory scope of the GDPR.[287]

The position could be different, however, for the use of commercial spyware services. At any rate where the service is designed such that personal data is actually transmitted to another body — specifically, the spyware vendor — a data processing relevant under data-protection law (preceding the actual spying-out of data) occurs. It is conceivable that this data processing has a bearing on the selection of specific vendors or on the decision to purchase a particular product. For the GDPR contains various rules that can already have effects on the design of data-processing systems: these include Art. 25 GDPR („data protection by design"), under which controllers „ shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, [...] which are designed to implement data-protection principles". Art. 28 GDPR, under which controllers may work only with processors that

---

[285] See also European Parliament, *Recommendation*, p 9-10; too broadly rejecting Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 284; this would impact the applicable fundamental rights framework, supra B.I.1.

[286] Of course, a vulnerability can later be exploited to obtain personal data through exploits. However, this process can and must then be assessed separately under data protection law.

[287] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 285.

provide „sufficient guarantees" that the data processing takes place in accordance with the provisions of the Regulation; Art. 32 GDPR, under which „appropriate technical and organisational means" must be taken to ensure data security; and Art. 35 GDPR, under which a so-called data-protection impact assessment must be carried out before particularly risky forms of data processing.

These requirements would, however, only have to be taken into account if no sectoral exception of the GDPR applies with regard to the drawing on private spyware capabilities.

Under Art. 2(2) point (d) GDPR, however, the Regulation does not apply to data processing by criminal-prosecution and police authorities. These are, at most, bound by the provisions of the Law Enforcement Directive.[288]

Under Art. 2(2) point (a) GDPR, the Regulation further does not apply to activities that „fall outside the scope of Union law". The CJEU does, admittedly, expressly want this exception provision to be understood narrowly.[289] In agreement with the predecessor provision, Art. 3(2) Directive 95/46, and Recital 16,[290] the CJEU, too, however, assumes that data processing by „ State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category," is not covered by the GDPR.[291] As activities aimed at safeguarding national security are in particular „those that are intended to protect essential State functions and the fundamental interests of society".[292] In its judgment on the French data-retention rules, the CJEU gave the concept still further contours. Here it held: "In that regard, it should be noted, at the

---

[288] Infra C.II.4.

[289] CJEU, Judgment of 22 June 2021, C-439/19, Rn. 62 (*Latvijas Republikas Saeima*) (with further references).

[290] „[...] Activities that do not fall within the scope of Union law, such as activities concerning national security ".

[291] CJEU, Judgment of 22 June 2021, C-439/19, Rn. 62-66 (*Latvijas Republikas Saeima*).

[292] CJEU, Judgment of 22 June 2021, C-439/19, Rn. 67 (*Latvijas Republikas Saeima*).

outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities".[293] To be distinguished from this are "the objectives of combating crime in general, even serious crime, and of safeguarding public security".[294]

Whether, by these standards, (all) intelligence activities of, for example, the Bundesnachrichtendienst or the constitutional-protection authorities can be assessed as concerning „national security" can ultimately be decided only by the courts. The high requirements of the CJEU, however, suggest that this cannot be affirmed across the board and for all areas of activity.

4. Law Enforcement Directive

The Law Enforcement Directive regulates the protection of natural persons with regard to the processing of personal data by public authorities acting for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Under the Law Enforcement Directive, too, the decision on how to handle a vulnerability does not constitute a processing of personal data,[295] so that here again only the drawing on external spyware capabilities is potentially contained. In this respect, the Law Enforcement Directive, too, contains rules that could already have a bearing on the purchase of a particular product, in

---

[293] CJEU, Judgment of 6 October 2020, C-511/18, Rn. 135 (*La Quadrature du Net ua*).

[294] CJEU, Judgment of 6 October 2020, C-511/18, Rn. 136 (*La Quadrature du Net ua*).

[295] See already supra C.II.3.

particular Art. 20 Law Enforcement Directive („data protection by design"), Art. 22 Law Enforcement Directive („processors"), and Art. 27 („data protection impact assessment").

The Law Enforcement Directive, too, however, again applies only to activities that fall within the scope of EU law, Art. 2(3) point (b) Law Enforcement Directive. Here, too, activities serving the protection of „national security" are therefore excluded.[296]

The ordinary activities of the criminal-prosecution and police authorities, which the Law Enforcement Directive is precisely intended to regulate, cannot, however — even where they concern serious forms of crime — be understood as concerning „national security".[297]

5. Cyber Resilience Act

With the Cyber Resilience Act, the European Union introduced uniform IT-security requirements for „products with digital elements" (e.g. software or IoT devices). Even though the Regulation accordingly addresses above all manufacturers and distributors of such products, it does also provide certain rights and duties for the Member States.

Specifically, under Art. 4(1), the Member States "shall not impede [...] the making available on the market of products with digital elements which comply with this Regulation". As Recital 13 of the Regulation also makes clear, however, the purpose of this provision is to prevent the enactment of additional cybersecurity requirements going beyond the Regulation. That it also seeks to prevent measures which may negatively affect the cybersecurity of products does not appear to be indicated.

Against the coverage of spyware „products" appears to speak that the Regulation, under Art. 2(7), is not to apply to „products with digital elements

---

[296] See also Rec 14 Law Enforcement Directive.

[297] See also supra C.I.2.

developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information", and that, under Art. 2(8), the „obligations laid down in this Regulation shall not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence".

IT vulnerability management, as well as the purchase of spyware, is therefore not affected by the Cyber Resilience Act.[298]

6. Cybersecurity Act

With the Cybersecurity Act, the EU strengthened, in 2019, the mandate of the European cybersecurity agency ENISA and laid down rules on its competences, on cooperation with national authorities, and on a uniform European certification framework. Requirements for IT vulnerability management or the purchase of spyware cannot, however, be derived from the Regulation.[299]

7. Result

In view of the uncertainties as to how far the sectoral exceptions created for the security authorities in primary and secondary law extend, it cannot be ruled out with certainty that individual provisions of the NIS 2 Directive, the ePrivacy Directive, the GDPR, and the Law Enforcement Directive have, in isolated respects, an influence on the state's handling of IT vulnerabilities and commercial spyware.

A comprehensive regulation of the questions affected here is not, however, currently found in EU law. This also means that EU law currently produces no

---

[298] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 286-288.

[299] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 286.

blocking effect in this respect for national rules on vulnerability management or on the purchase of spyware.

III. Distribution of Competences within the German Federal System

Within Germany, legislative competence is governed by Art. 70 et seq. Grundgesetz. Under the basic rule of Art. 70(1) Grundgesetz, the Länder in principle have the right to legislate, insofar as the Grundgesetz does not expressly confer legislative competences on the Federation. The Grundgesetz does so above all in Articles 73 and 74 Grundgesetz, which confer exclusive (Art. 73 Grundgesetz) and concurrent legislative competences (Art. 74 Grundgesetz) on the Federation.

A federal competence to regulate vulnerability management and spyware purchase by the federal security authorities follows already from the Federation's competence to regulate the exploitation of vulnerabilities by these authorities.[300] Specifically, this concerns the BND (Art. 73(1) no. 1 Grundgesetz), the MAD (Art. 73(1) no. 1 var. 2 Grundgesetz), the BKA (Art. 73(1) nos. 9a, 10 Grundgesetz), and the Bundespolizei (Art. 87(1) sentence 2 in conjunction with Art. 73(1) no. 5 Grundgesetz).[301]

For the regulation of the handling of vulnerabilities by other federal authorities, there is an unwritten legislative competence arising from the nature of the matter[302] or from factual connection.[303] For vulnerability

---

[300] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 214 f.

[301] Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, p 35 (50 ff.).

[302] See also the legislative history regarding NIS-2-UmsuCG, Deutscher Bundestag, *Drucksache 21/1501*, p 98.

[303] Wischmeyer, in: Dreier, Grundgesetz, 4. Aufl., Art. 70 Rn. 58 f. see also for similar situations BVerfG, Judgment of 2 March 2010 - 1 BvR 256/08; BVerfG, Order of 24 Jaunary 2012 -1 BvR 1299/05; BVerfG, Order of 8 October 2024 - 1 BvR 1743/16, 1 BvR 2539/16, Rn. 149 (*BND-Cybergefahren*).

management and spyware purchase by the criminal-prosecution authorities, it arises from the competence for judicial procedure, Art. 74(1) no. 1 Grundgesetz.[304]

It is then questionable whether the Federation may, beyond this, also make rules for Länder authorities on the handling of vulnerabilities or commercial spyware capabilities.

The Grundgesetz does not recognize a uniform head of competence for the regulation of information security.[305] The federal legislature assumes, however, that at any rate the current nationwide IT-security requirements of the BSI Act for critical facilities and so-called important and particularly important entities can be based — alongside sectoral regulatory competences (for example, for telecommunications under Art. 73(1) no. 7 Grundgesetz) — also on the competence to regulate the law of the economy under Art. 74(1) no. 11 Grundgesetz.[306] The necessity of a federal statutory regulation to preserve economic unity in the overall state interest under Art. 72(2) Grundgesetz is also said to be given, in view of the increased threat situation, because of otherwise imminent „ significant distortions of competition".[307]

A regulation of vulnerability management or of spyware purchase cannot, however, probably be based on the competence to regulate economic law. For even though IT vulnerabilities obviously have (large) economic effects,[308] they are, first and foremost, matters to be assigned to the field of „threat prevention".[309]

---

[304] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, 214 f.

[305] See also Wischmeyer, *Informationssicherheit*, 2023, p 164.

[306] Deutscher Bundestag, *Drucksache 21/1501*, p 97 f.

[307] Deutscher Bundestag, *Drucksache 21/1501*, p 97 f.

[308] See also B.I.6.

[309] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 215 (with further references); see also Kipker, *IT-SiG 2.0: Kompetenzgerangel zwischen Bund und Ländern* (09.02.2021), Beck Blog.

A number of further heads of competence come into consideration, however, in particular Art. 73(1) no. 10 var. 1 Grundgesetz in conjunction with Art. 87(1) sentence 2 Grundgesetz: under Art. 73(1) no. 10 var. 1 Grundgesetz, the Federation may make rules for the „cooperation between the Federation and the Länder concerning (a) criminal police work, [and] (b) protection of the free democratic basic order, existence and security of the Federation or of a Land (protection of the constitution)". Institutionally, the cooperation can also be organized via so-called central offices, to whose establishment in certain fields Art. 87(1) sentence 2 Grundgesetz grants authorization.[310]

According to the definition of the Constitutional Court, „Zusammenarbeit" means „the ongoing mutual provision of information and disclosure, mutual consultation, and mutual support and assistance within the limits of each authority's own powers[, as well as] functional and organisational links, joint facilities, and shared information systems".[311] As this definition already suggests, the core of cooperation lies in the creation of common (communications) infrastructures, facilities, and resources.

It is, however, also discussed whether the competence (in exceptional cases) also permits the Federation to grant the Länder substantive powers of interference,[312] to oblige the Länder to equip their authorities with certain powers,[313] to oblige the Länder to create the framework conditions necessary

---

[310] Art. 87 Abs. 1 Satz 2 Grundgesetz „By federal law, federal border protection authorities, central offices for police information and intelligence services, for criminal police purposes and for the collection of documents for constitutional protection purposes [...] can be established."; regarding the relationship between Article 73(1)(10) variant 1 Basic Law in conjunction with Article 87(1) sentence 2 Basic Law, Dürig/Herzog/Scholz/*Ibler* (August 2025) Art. 87 Grundgesetz Rn. 117-120.

[311] BVerfG, Order of 10 November 2020 - 1 BvR 3214/15, Rn. 76 (*Antiterrordateigesetz II*); BVerfG, Judgment of 24 April 2013 - 1 BvR 1215/07, Rn. 97 (*Antiterrordateigesetz I*).

[312] Answering in the negative Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, p 35 (58 ff.); Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 Grundgesetz Rn. 235.

[313] Answering in the negative Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich,

for cooperation,[314] to grant the Federation powers of instruction vis-à-vis Länder authorities in cases of conflict,[315] or even to act in place of the Länder.[316]

The purpose of the competence norm actually suggests an application to vulnerability management — whose particular need for coordination is triggered, in particular, by the fact that a once-disclosed vulnerability is burned for all potential official users.[317][318]

In the result, however, it would amount to an erosion or transfer of Länder competences no longer covered by Art. 73(1) no. 10 Grundgesetz if the Federation were to oblige the Länder to conduct vulnerability management or to make obligatory use of a nationwide centralized procedure for this purpose.[319]

Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, p 35 (58 ff.); Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 Grundgesetz Rn. 235; BeckOK Grundgesetz/*Seiler* (November 2025), Art. 73 Grundgesetz Rn. 46.3.

[314] Approving Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 Grundgesetz Rn. 233

[315] Restrictive Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, p 35 (65 ff.). Affirmatively, but limited to purposes of coordination, Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 Grundgesetz Rn. 234 ("provided that this is suitable and necessary with regard to the intended purpose of coordination and is compatible with the requirement of considerate treatment of state authorities"); under current law, such powers of instruction are granted both to federal central offices, specifically: the BKA (§ 4 BKAG), and to the Federal Government, specifically: in § 7 BVerfSchG.

[316] Affirmatively, but subject to an express constitutional authorization, Dürig/Herzog/Scholz/*Uhle* (August 2025) Art. 73 Grundgesetz Rn. 231. Also rejecting sectoral centralization de constitutione lata Wischmeyer, Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, p 35 (71 ff.).

[317] Just as a concealed vulnerability will regularly pose dangers to persons and institutions whose protection is the responsibility of authorities at a different territorial level.

[318] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 217-218.

[319] See also Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 219.

It is possible, however, for the purposes of cooperation, to permit the Länder the optional use of a vulnerability-management process established at the federal level, and moreover to provide, by federal-law order — herein lies the core of the central-office function — for reciprocal duties of participation and information.[320] This would mean that the Federation cannot oblige Länder authorities to conduct vulnerability management according to certain requirements, but that the Länder (and also the Federation) can be obliged, in the event that a vulnerability-management process is established, to involve the respective other level of government in the decision-making procedure. This could be ensured, for example, through an opportunity to submit observations in the decision-making procedure or a right to be informed about discovered and secretly kept vulnerabilities.

Art. 91c(1) Grundgesetz further comes into consideration, which permits the Federation and the Länder „to specify the standards and security requirements necessary for exchanges between their information technology systems". However, the norm contains no legislative competence of the Federation.[321] Rather, it merely establishes that federal cooperation in the area of IT systems — for example, through state treaties or administrative agreements — is permitted. Moreover, the norm covers only the planning, establishment, and operation of IT infrastructure. Powers of action or cooperation going beyond such technical questions are not to be allocated by the norm.[322] Accordingly, Art. 91c(1) Grundgesetz empowers the Federation neither to oblige Länder authorities to conduct vulnerability management, nor to make requirements for them on the deployment of commercial spyware.

---

[320] Similarly Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 216-220; However, the thesis that the federal government may "establish uniform criteria and minimum standards for deciding how to deal with IT security gaps" probably goes too far, Buntrock, *Staatlicher Umgang mit IT-Sicherheitslücken*, 2025, p 220.

[321] Unlike Articles 91c(4) and (5) of the Basic Law, which, however, are not relevant to the questions at issue here.

[322] See also Dreier Band III/*Heun/Thiele* (2018) Art. 91c Rn. 8 ff.

The Federation therefore has a legislative competence to regulate the handling of IT vulnerabilities and the purchase of spyware by the federal authorities, but not by the Länder authorities. Beyond this, the Federation could oblige the Länder to take certain cooperation measures in these fields.

Legislative Proposal

As expressed in the analysis above, the Grundgesetz requires a regulation of vulnerability and spyware management by formal statute that covers certain minimum aspects.

This constitutionally required minimum would be met by the following legislative proposal.

Within this framework, however, the federal legislature has certain latitude for decision, in particular as regards the selection and design of the decision-making and the control body. The following legislative proposal assumes that the legislature decides, in this respect, to create a new decision-making body („Vulnerability Management Panel“) which, together with its secretariat, is located at the Federal Chancellery and is subject to control by the Unabhängiger Kontrollrat. These are, however, decisions which, according to the foregoing analysis, are well justifiable but not constitutionally mandatory, and rather lie within the legislature's discretion. This is marked in the text by [square brackets around these optional regulatory aspects, which require completion].

§ 1 Vulnerability Management

(1) [1]Authorities and other public bodies of the Federation are obliged to report vulnerabilities that become known to them within the meaning of § 2 no. 38 BSIG, which are unknown to the vendor of the affected product and to the public, to the vendor of the affected product. [2]To this end, the authority or other public body shall report the vulnerability to the Federal Office for Information Security for the purpose of coordinated disclosure under Article 12(1) of the NIS 2 Directive. [3]If the authority is of the view that the vulnerability should exceptionally be kept secret owing to an overriding countervailing public interest, it shall without delay refer the vulnerability to

the regulated procedure for deciding on the secrecy of a vulnerability under paragraph 3. [4]This applies regardless of the origin of the knowledge. [5]Exempt from the obligation under sentence 3 are vulnerabilities reported to the authority or other public body exclusively for the purpose of coordinated disclosure, as well as cases of urgent danger requiring immediate action.

(2) [1]Responsible for the decision on the secrecy of a vulnerability is [the Vulnerability Management Panel]. [[2]The Panel is composed of representatives of the Federal Ministries of the Interior; of Defence; for Economic Affairs and Energy; of Justice and for Consumer Protection; and for Digital Affairs and State Modernization; as well as of the Federal Chancellery, the Federal Office for Information Security, the Central Office for Information Technology in the Security Sphere, the Federal Office for the Protection of the Constitution, the Bundesnachrichtendienst, the Military Counterintelligence Service, the Bundeskriminalamt, the Bundespolizei, the Bundeswehr, and the Federal Office of Civil Protection and Disaster Assistance. [3]It is supported in its work by a secretariat located at the Federal Chancellery. [4]The Panel shall take its decisions by consensus.]

(3) [1]For the decision on how to handle the vulnerability, the competing interests — in particular the dangers threatened by keeping the vulnerability secret and the benefit of a possible state use of the vulnerability — are to be weighed against one another. [2]As a rule, the decision shall be for disclosure of the vulnerability; disclosure may be refrained from only where, in the individual case, the interest in secrecy prevails. [3]The procedure shall be designed such that an appropriate and timely decision is ensured.

(4) [1]The following consequences of the decision come into consideration:

1. reporting the vulnerability to the vendor by way of a coordinated procedure under Article 12(1) of the NIS 2 Directive;
2. temporary secrecy;
3. the passing-on of risk-mitigating information without full disclosure;
4. the restriction of use by state bodies; as well as
5. the confidential passing-on to other authorities.

[2]Vulnerabilities kept secret are to be re-examined regularly and disclosed as soon as the conditions for their secrecy no longer apply.

(5) For the storage and processing of information about vulnerabilities, heightened information-security requirements apply, which must correspond to the respective state of the art.

(6) [1]Decisions on secrecy are subject to independent control by [the Unabhängiger Kontrollrat]. [2]The decisions, together with their underlying considerations, are to be submitted to [the Unabhängiger Kontrollrat], and all information necessary for the control is to be provided. [3]The Parlamentarisches Kontrollgremium is to be informed of the decisions.

(7) [1]The decisions of the [Vulnerability Management Panel] are to be documented. [2]The extent and manner of the handling of vulnerabilities are to be reported publicly at regular intervals in an appropriate manner.

(8) The details, in particular concerning the procedure, the balancing criteria, and the security requirements, are to be regulated by ordinance of the Federal Government.

§ 2 Use of External Cyber Capabilities

(1) Authorities and other public bodies of the Federation may draw on external cyber capabilities, in particular from private vendors or foreign security authorities, only insofar as this is necessary for the performance of their statutory tasks and the use is not excluded by statute.

(2) [1]Before the procurement or use of external cyber capabilities, a structured examination and decision-making procedure is to be carried out by the [Vulnerability Management Panel]. [2]In this procedure, at least the following are to be examined:

a) the compatibility of the use of the external cyber capabilities with applicable law, in particular with data-protection requirements;
b) the dangers that the external cyber capabilities pose to information-technology security, in particular through exploited or kept-open vulnerabilities;

c) the trustworthiness of the vendor, including its supply chains and investors;
d) the danger of further dissemination or misuse of the deployed technologies;
e) the risk of intelligence-service influence or other security-endangering dependencies;
f) the vendor's compliance with rule-of-law minimum standards, in particular as regards the exclusion of deliveries to states or actors that do not observe fundamental rule-of-law principles.

(3) [1]The assessment is to be carried out on the basis of reliable, current, and verifiable information. [2]It is to be fully documented and continuously updated. [3]The vendors are to be obliged to cooperate, in particular to disclose relevant information. [4]Use is impermissible where the risks under paragraph 2 cannot be sufficiently controlled.

(4) Vis-à-vis private vendors, compliance with statutory requirements is to be secured through contractual arrangements and appropriate sanction mechanisms.

(5) Compliance with the requirements under paragraphs 2 to 4 is subject to independent control by [the Unabhängiger Kontrollrat].

(6) The details, in particular concerning the procedure and the examination criteria, are to be regulated by ordinance of the Federal Government.

Bibliography

Bernsen, Winnona DeSombre (2024), Crash (exploit) and burn: Securing the offensive cyber supply chain to counter China in cyberspace, abrufbar unter https://www.atlanticcouncil.org/in-depth-research-reports/report/crash-exploit-and-burn/.

Bundesamt für Sicherheit in der Informationstechnik (2022), Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess (01.12.2022), abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.pdf

Bundesministerium des Innern, für Bau und Heimat (2021), Cybersicherheitsstrategie für Deutschland 2021, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=2.

Calliess, Christian/Baumgarten, Ansgar (2020), Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective, *German L. J.* 21 (2020), S. 1149.

Calliess, Christian/Ruffert, Matthias (2022), TEU • TFEU (6. Auflage), C.H. Beck München.

Deibert, Ron (2026), The Perils of Privatized Cyberwarfare, *Lawfare* (01.04.2026), abrufbar unter https://www.lawfaremedia.org/article/the-perils-of-privatized-cyberwarfare.

Deutscher Bundestag (2015), Drucksache 21/1501.

Dreier, Horst (Hrsg.) (2018), Grundgesetz-Kommentar. Band III: Artikel 83-146 (3. Auflage), Mohr Siebeck Tübingen.

Dürig, Günter/Herzog, Roman/Scholz, Rupert (Hrsg.) (2025), Grundgesetz (108. Auflage), C.H. Beck München.

Epping, Volker/Hillgruber, Christian (Hrsg.) (2025), BeckOK Grundgesetz (63. Edition), C.H. Beck München.

European Parliament (2023), Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation) (P9_TA(2023)0244).

Executive Office of the President (2023), Executive Order 14093 - Prohibition on Use by the United States Government of Commercial Spyware That Poses Risks to National Security (27.03.2023).

FIRST.Org, Inc. (2024), Common Vulnerability Scoring System Version 4.0: Specification Document (Version 1.2), abrufbar unter https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf.

Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus/Kirchmair, Lando (2023), TEU/TFEU (7. Auflage), C.H. Beck München.

Google Threat Analysis Group (2024), Buying Spying, abrufbar unter https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.) (2025), Das Recht der Europäischen Union. Band I TEU/TFEU (85. EL), C.H. Beck München.

Herpig, Sven/Schwartz, Ari (2023), The Future of Vulnerabilities Equities Processes Around the World, *Lawfare* (4. Januar 2023) abrufbar unter https://www.lawfaremedia.org/article/future-vulnerabilities-equities-processes-around-world.

Herpig, Sven (2018), Schwachstellen-Management für mehr Sicherheit, abrufbar unter https://www.interface-eu.org/storage/archive/files/vorschlag.schwachstellenmanagement.pdf.

Kipker, Dennis-KenLaw Enforcement (2021), IT-SiG 2.0: Kompetenzgerangel zwischen Bund und Ländern, Beck Blog (09.02.2021), abrufbar unter https://intrapol.org/2021/02/09/it-sig-2-0-kompetenzgerangel-zwischen-bund-und-laendern/.

Krempl, Stefan (2023), Trotz Verbot: FBI hat über Vertragsfirma NSO-Spyware finanziert, Heise Online (31.07.2023), abrufbar unter https://www.heise.de/news/Trotz-Verbot-FBI-hat-ueber-Vertragsfirma-NSO-Spyware-finanziert-9231066.html.

Meister, Andre (2022), Staatstrojaner Pegasus wird alle 40 Minuten eingesetzt, Netzpolitik (22.06.2022), abrufbar unter https://netzpolitik.org/2022/pega-untersuchungsausschuss-staatstrojaner-pegasus-wird-alle-40-minuten-eingesetzt/.

Panagiotopoulos, Vas (2026), Policymakers Ignore Spyware Middlemen Driving Global Proliferation, Tech Policy Press (18.03.2026), abrufbar unter https://www.techpolicy.press/policymakers-ignore-spyware-middlemen-driving-global-proliferation/.

Roberts, Jen/Herr, Herr/Bansal, Nitansha/Messieh, Nancy (2024), Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights, abrufbar unter https://www.atlanticcouncil.org/wp-content/uploads/2026/03/Mythical-Beasts-Cyber-Statecraft.pdf.

Sandhu, Aqila (2024), Squaring the Circle: The CJEU between Fundamental Rights Guardian and Architect of a Security Union, *Verfassungsblog* (02.12.2024), abrufbar unter https://verfassungsblog.de/squaring-the-circle-data-retention/.

Smally, Suzanne (2024), Testimony from NSO Group raises questions about its culpability for spyware abuses, The Record (19.11.2024), abrufbar unter https://therecord.media/nso-group-whatsapp-case-documents.

SPD (2021), Koalitionsvertrag 2021-2025, abrufbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

Streinz, Rudolf (Hrsg.) (2018), TEU/TFEU (2. Auflage), C.H. Beck München.

The Citizen Lab (2026), Submission of the Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto, to the United Nations

Working Group on the Use of Mercenaries, abrufbar unter https://citizenlab.ca/wp-content/uploads/2026/04/CitLab-Submission-to-the-UN-WG-on-the-use-of-mercenaries.pdf.

Tzanou, Maria/Vogiatzoglou, Plixavra (2025), National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach, *European Papers eJournal* (18.11.2025).

U.S. Department of Commerce (2021), Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (03.11.2021) abrufbar unter https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

U.S. Government (2017), Vulnerabilities Equities Policy and Process for the United States Government (15.11.2017), abrufbar unter https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/external%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

Wischmeyer, Thomas (2020), Der Verfassungsschutzverbund: Verfassungsrechtliche Rahmenbedingungen und Entwicklungsperspektiven, in: Dietrich, Jan-Hendrik et al. (Hrsg.), *Nachrichtendienste in vernetzter Sicherheitsarchitektur*, S. 35 .

Wischmeyer, **Thomas** (2023), Informationssicherheit, Mohr Siebeck Tübingen.

Wischmeyer, Thomas (2024), Staatliche Nutzung von IT-Sicherheitslücken – Grundzüge des staatlichen Schwachstellenmanagements, in: Raue, Benjamin (Hrsg.), *Digitale Resilienz: Effektives Recht auf sichere Software (Band II).*

Table of Authorities

BVerfG, Order of 10 November 2020 – 1 BvR 3214/15 (*Antiterrordateigesetz II*)

BVerfG, Order of 24 March 2021 – 1 BvR 2656/18 (*Klimaschutzgesetz*)

BVerfG, Order of 8 June 2021 – 1 BvR 2771/18 (*IT-Sicherheitslücken*)

BVerfG, Order of 20 January 2022 – 1 BvR 1552/19 (*Hessentrojaner*)

BVerfG, Judgment of 26 April 2022 – 1 BvR 1619/17 (*Bayerisches Verfassungsschutzgesetz*)

BVerfG, Order of 8 October 2024 – 1 BvR 1743/16, 1 BvR 2539/16 (*BND-Cybergefahren*)

BVerfG, Order of 24 June 2025 – 1 BvR 2466/19 (*Trojaner I*)

BVerfG, Order of 24 June 2025 – 1 BvR 180/23 (*Trojaner II*)

Court of Justice of the European Union

CJEU, Judgment of 2 May 2006, C-217/04 (*ENISA*)

CJEU, Judgment of 4 March 2010, C-38/06 (*Commission/Portugal*)

CJEU, Judgment of 10 June 2014, C-198/13 (*Julian Hernández et al*)

CJEU, Judgment of 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige*)

CJEU, Judgment of 20 March 2018, C-187/16 (*Commission/Austria*)

CJEU, Judgment of 2 October 2018, C-207/16 (*Ministerio Fiscal*)

CJEU, Judgment of 22 January 2020, C-177/18 (*Baldonedo Martín*)

CJEU, Judgment of 6 October 2020, C-511/18 (*La Quadrature du Net*)

CJEU, Judgment of 6 October 2020, C-623/17 (*Privacy International*)

CJEU, Judgment of 22 June 2021, C-439/19 (*Latvijas Republikas Saeima*)

CJEU, Judgment of 20 September 2022, C-793/19 and C-794/19 (*SpaceNet*)

CJEU, Judgment of 30 March 2023, C-34/21 (*Hauptpersonalrat*)

CJEU, Judgment of 30 April 2024, C-470/21 (La Quadrature du Net)