2

Conceptualising the Protected Interests in Data Protection Law

MARION ALBERS

I. Introduction

How to conceptualise the interests of individuals to be protected with respect to the handling of personal data and information is a key issue in the development of information and data law. The more society becomes digitalised, data-driven, and dependent on cross-border data flows, the more attention is drawn to this area of law.[1] However, the approaches taken are very different, not least when comparing Europe and the US. At the same time, approaches are in a state of flux, and fresh ideas are needed. This chapter argues that data protection addresses a highly complex subject matter with its own set of characteristics. Therefore, it must be conceived as a novel, distinct facet of fundamental rights protection. More precisely, based on a functional cooperation of fundamental rights at different levels, data protection comprises a bundle of multi-layered, multi-dimensional, and multi-faceted provisions and rights to which all fundamental rights can contribute with their substantive particularities. Against this background, the 'right to the protection of personal data' now enshrined in some fundamental rights catalogues proves to be a fruitful, although not indispensable, step forward as a pillar to be developed in an interplay with other fundamental rights.

My contribution will first provide a brief overview of the backgrounds (II.). The idea of data protection has, to some extent, evolved from the idea of privacy. But it is also distinct from it. In today's environment – the Internet, digitalisation, AI – we are dealing with digital data, and I will introduce the essential understanding of data and personal data in the context of data protection law to provide the foundations for further considerations. We will then take a look at the familiar but fuzzy concepts of the right to privacy, the right to informational self-determination, and the right to the protection

[1] See the manifold articles in M Albers and IW Sarlet (eds), *Personality and Data Protection Rights on the Internet* (Dordrecht, Springer (Ius Gentium), 2022).

of personal data (III.). The analysis of both the backgrounds and the achievements and limitations of these different concepts leads to my own approach (IV.). Data protection deals with a highly complex distinct subject matter, and any sufficiently well-thought-through legal approach points to multi-layered, multi-dimensional, and multifaceted guarantees and rights as well as to sophisticated doctrinal constructions. These insights enable us to comprehend the protected interests of data subjects as a bundle of provisions and rights in a multi-layered approach that includes, at a basic level, provisions and rights for appropriate regulation, and, at a second level, further requirements arising from content-specific fundamental rights. Such an approach is a prerequisite for developing data protection law in a reasonable way and for coordinating it with other legal regulations, for example, with the overarching European data and digital strategy. The chapter closes with a summary and an outlook (V.).

II. Backgrounds

A. Data Protection in the Digitalised Society

The idea of data protection has some of its roots in the idea of privacy, and this concept in turn has a very colourful history. Its traditional understanding has been shaped by several guiding dichotomies:[2] the contrasting of privacy and the state,[3] the distinction between privacy and publicness,[4] and the differentiation between the individual's private matters and the spheres of decision and influence (also) open to others.[5] A closer scrutiny quickly reveals the numerous premises and the complexity of the converse terms. Nonetheless, a basic understanding emerges: 'Privacy' assigns something to a person or a group of persons as their own concern and establishes limits to others' access to it. Over time, and more controversially, the range of issues that privacy addresses,[6] the mechanisms of allocation as one's own, and the concept of access have been understood in an increasingly abstract and broad way. Topics include personal communications, documents and data, 'access' comprises informational

[2] *Cf* M Albers, 'Privatheitsschutz als Grundrechtsproblem' in S Halft and H Krah (eds), *Privatheit. Strategien und Transformationen* (Passau, Stutz, 2013) 15 (20).

[3] This dichotomy is constitutive for liberal thought. *Cf* B Rössler, *Der Wert des Privaten* (Frankfurt am Main, Suhrkamp, 2001) 27 ff.

[4] The concept of 'publicness' is conceived in a variety of ways. See J Weintraub, 'The Theory and Politics of the Public/Private Distinction' in J Weintraub and K Kumar (eds), *Public and Private in Thought and Practice. Perspectives on a Grand Dichotomy* (Chicago, University of Chicago Press, 1997) 1 (1 ff); N Bobbio, 'The Great Dichotomy: Public/Private' in N Bobbio, *Democracy and Dictatorship* (Cambridge, Polity Press, 1989) 1 (17). *Cf* also with criticism R Geuss, *Public Goods, Private Goods* (Princeton, Princeton University Press, 2001).

[5] This differentiation is linked to one's individuality, but is not identical to it.

[6] Varying across cultures and historical epochs, the range of issues include the body, facets of the personality, religious convictions and conscience, spaces such as place of residence, property, close relationships such as partnership and family, confidential documents, communications only to specific addressees, or personal data. *Cf* with a broad historical overview the contributions in P Ariès et al, *Histoire de la vie privée*, (Paris, Seuil, 1985–1987). *Cf* also R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 440 ff.

measures,[7] and 'limits to access' extend to boundaries based on social expectations of expectations.[8]

When the idea of data protection began to emerge in the 1960s and 1970s, privacy discourses already provided a variety of starting points. Moreover, in a more or less clear distinction from these, data protection was initially conceived with concepts of its own that not only emphasised the relevance of all individual rights but also considered the institutional or societal handling of (personal) data as such in need of regulation.[9] The socio-technical stimulus – automated data processing in large computer systems – could certainly have created the conditions for the development of overarching regulatory concepts. But the first attempts at a complex regulation quickly took a turn towards an individual-rights approach. One of the reasons for this was particular references to the discourses on privacy, which for their part have been specifically narrowed down. For example, in 1972, Wilhelm Steinmüller and other German scholars proposed an individual-rights-orientated, phase-specific approach to data protection,[10] following Westin's idea to define the right to privacy as 'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[11] From the Federal Constitutional Court's census ruling in 1983 onwards, data protection and its principles have been significantly influenced by the right to informational self-determination.

Since the beginning of the current millennium, we have been experiencing a very profound social change that extends to ontologies. This change is once again prompted by novel socio-technical arrangements, particularly in connection with the internet as an infrastructure, digitalisation, and AI. Areas of life are subject to datafication, activities are becoming data-driven, and communications are characterised by 'virtual contingency'[12] due to the autonomous contribution of machine data processing. In response to this societal change, a series of new regulations of data, technologies and infrastructures enters the scene. In Europe, this is the European Union's data and digital strategy for 'shaping Europe's digital future'.[13]

[7] See the description of 'privacy' by S Bok, *Secrets – On the Ethics of Concealment and Revelation* (New York, Pantheon Books, 1982) 10 f: 'the condition of being protected from unwanted access by others – either physical access, personal information, or attention'.

[8] *Cf* H Nissenbaum, *Privacy in Context. Technology, Policy, and the Integrity of Social Life* (Stanford, Stanford University Press, 2010) 74 ff.

[9] See G González Fuster, ch 6 in this volume. For the early discussion in Germany see M Albers, *Informationelle Selbstbestimmung* (Baden-Baden, Nomos, 2005) 113 ff.

[10] W Steinmüller et al, *Grundfragen des Datenschutzes*, Bundestags-Drucksache VI/3826 (1972). Admittedly, this approach was part of an overarching concept in that expertise, but the overarching elements have been lost in subsequent developments. See F Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law* (The Hague, TM Asser Press, 2022) 180 ff.

[11] AF Westin, *Privacy and Freedom*, 6th edn (New York, Atheneum, 1970) 42.

[12] See E Esposito, 'Artificial Communication? The Production of Contingency by Algorithms' (2017) 46(4) *Zeitschrift für Soziologie* 249 (257 ff).

[13] For the foundations see in particular: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'European Interoperability Framework – Implementation Strategy' [2017] COM(2017) 134 final; 'Towards a common European data space' [2018] COM(2018) 232 final; 'Shaping Europe's digital future' [2020] COM(2020) 67 final; 'A European strategy for data' [2020] COM(2020) 66 final; 'European Commission digital strategy. Next generation digital Commission' [2022] COM(2022) 4388 final; White Paper 'On Artificial Intelligence – A European approach to excellence and trust' [2020] COM(2020) 65 final.

This strategy covers the regulations on digital markets and digital services,[14] the regulation on a framework for the free flow of non-personal data,[15] open data concepts,[16] the Data Governance Act[17] and common European sector-specific data spaces[18] that, among other things, create a framework for 'data altruism',[19] the Data Act that revolves around ensuring that personal and non-personal data generated in the context of the Internet of Things is made available for use by various stakeholders,[20] and, last but not least, harmonised rules on artificial intelligence.[21] Some of these new regulations come along with new principles such as data sharing or making data available for their reuse in various contexts. Actually, they are fuelling pressure for change on the familiar data protection regulations.[22] Nevertheless, these are classified

[14] Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L265/1; Regulation (EU) 2022/2065 of the European Parliament and of the Council on a single market for digital services (Digital Services Act) [2022] OJ L277/1. Their provisions concern the regulation of gatekeepers including their handling of data or obligations of online platforms, for example, with regard to user-generated illegal content. In addition, the aim of these strategies is to establish a common European data space or sector-specific data spaces, the design of which is intended to unlock the potential of digitisation.

[15] See Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59, and the Commission's Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union (2019), which in particular deal with the demarcation from the regulations on personal data in the GDPR [2019] COM(2019) 250 final.

[16] The respective regulations aim to ensure that certain data sets and documents in the public sector are made available in open, machine-readable, accessible, findable and reusable formats, and may be reused in the private sector, subject to conditions if necessary; see Directive 2019/1024/EU of the European Parliament and of the Council on open data and the re-use of public sector information [2019] OJ L172/56; for delimitation in the above context, see art 2(1)(h) on its scope.

[17] Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L152/1.

[18] See, eg, the intended Regulation on the European Health Data Space in its last version of the draft after consensus has been reached in the trilogue procedure, European Parliament legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the European Health Data Space ([2024] COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), www.europarl.europa.eu/doceo/document/TA-9-2024-0331_EN.html.

[19] Data subjects provide data for specified (research) purposes by means of consent. Complementing the Open Data Directive, the reuse of sensitive data is facilitated under certain conditions, first of all through the implementation of technological data protection concepts. New institutions such as data intermediaries, ie, data sharing services that can also operate in the sense of 'data trustees', and data altruistic organisations are given a key role with regard to, among other things, ensuring data protection rights.

[20] See the Regulation 2023/2854/EU of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) [2023] OJ L1/71. To achieve this goal, data owners must adhere to and ensure certain conditions for data processing. Above all, users of products or related services are to be enabled to use the data that is generated by their use (user-generated data), to share it with third parties or demand direct access for third parties. Subject to the specified criteria, data access is opened up for the benefit of public bodies. All in all, the knowledge and value creation potential of this data shall be exploited in a productive manner.

[21] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence […] (Artificial Intelligence Act) [2024] OJ L, 12.7.2024.

[22] These include above all the General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 – which is supplemented by the Data Protection Directive for Police and Criminal Justice – Directive 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

as a first fundamental pillar intended to provide a 'framework for trust in the digital environment'.[23] Personal data is explicitly a key factor upon which the legal regimes are built and are delineated. Let us now take a brief look at this core element of data protection: personal data.

B. Personal Data in Context

i. What is Data?

Although personal data is a core element of data protection, it is far from sufficiently clear what the concept of data is and what is or is not covered by it. Therefore, I am briefly introducing the subject matter in order to lay the foundation for further considerations.

The etymological root, with regard to which data presents itself as something 'given', creates an extraordinarily broad starting point for the understanding of the term 'data', and this understanding varies according to historical epoch, perspective, and framing. Data is a construction[24] and 'sociotechnological in nature',[25] because it, its storage forms, and the data formats in which data is embodied are shaped by technologies, media, and infrastructures. While in a certain phase 'data' was often linked to the evolution of science, experimentation, and measurement,[26] today they are a multifaceted element of the 'onlife world' as binary digital units which are, depending on the technology, manifested in dual electrical, optical or electromagnetic (voltage or light) states.

No surprise, modern approaches choose a very abstract level:

> […] the general definition of a datum is: Dd) datum = def. x being distinct from y, where x and y are two uninterpreted variables and the relation of 'being distinct', as well as the domain, are left open to further interpretation.[27]

This seems to be too abstract to be useful. But such an approach can capture different levels of abstraction and different reference points. Such a highly abstract approach is also necessary and suitable for grasping 'digital data' against the background of digitalisation and AI.

As the concept of data is a construction, the various scientific disciplines each take their own approach. Concepts of 'data' are described in multifarious and discipline-dependent ways.[28] The law does not simply borrow descriptions like those approaches in

[2008] OJ L119/89, by the e-privacy Directive – Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, and by numerous further sector-specific legal acts.

[23] Communication from the Commission 'Towards a common European data space' [2018] COM(2018) 232 final, p 1.

[24] R Kitchin, *The Data Revolution* (Los Angeles, Sage, 2014) 2 ff; S Leonelli, 'The Philosophy of Data' in L Floridi (ed), *The Routledge Handbook of Philosophy of Information* (London, Routledge, 2016) 192 (192 ff).

[25] R Kitchin, *Data lives: How Data are Made and Shape our World* (Bristol, Bristol University Press, 2021) 5.

[26] *Cf* also D Rosenberg, 'Data before the Fact' in L Gitelman (ed), *"Raw Data" is an Oxymoron* (Cambridge (MA), MIT Press, 2013) 33 (36).

[27] L Floridi, *Information. A Very Short Introduction* (Oxford, Oxford University Press, 2010) 23.

[28] ibid 19 ff.

computer science might use. Instead, it builds on different types of description patterns to cover the spectrum of regulatory needs and cases, takes them up in a legally specific way, and reformulates them with a view to the legally justified need for protection. What is meant by 'data' in the juridical context is, to a certain extent, a legal construction in itself. Since the concept of data is such an abstract one, there may be different descriptions even in different areas of law, such as data protection law, copyright law, or patent law. For example, we have different legal definitions in the GDPR on the one hand[29] and in the Data Governance Act and Data Act on the other[30] – all of them not well thought through, but not necessarily inconsistent, because they can be explained from their specific legal context.

ii. Data in Data Protection Law

The aim of data protection law is not the protection of data but of the persons to whom the data refers. This is reflected in its focus on 'personal data'.[31] How data is to be understood in data protection law must be approached by simultaneously considering 'personal data'.

Personal data is understood as data concerning the individual.[32] That means that its content refers to a particular natural or, depending on the legal system, also other legal person. However, such content is neither an intrinsic property of data nor is it attached to it like a label. It is an achievement attributing meaning to data. Two key questions are hidden in the 'person-relatedness': When does data refer to a *specific* person, and when does data *refer* to a person?

Data protection law responds by defining that the data must relate to either an identified or an identifiable person.[33] Data such as the personal name and data that is regularly linked to it, such as the address, date of birth, marital status, social security and tax identification numbers, fingerprints, or portrait photographs, are illustrative examples. Even with these simple examples, it quickly becomes clear that it must be answered which identifiers specify a person and that, if necessary, a connection between particular data and identification data must be drawn. Such a connection may be readily available in a given situation, but it may also only be possible by means of a number of steps, the relevance of which must be legally assessed with regard to the identifiability of a person. Prior or additional knowledge that some people might have can enable them to associate data that is not readily assignable on its own with a specific person.[34] If a reference to the person to be protected can only be established via

[29] Art 4 no 1 GDPR: '"personal data" means any information relating to an identified or identifiable natural person ("data subject") […]'.

[30] Art 2 no 1 DGA and 2 no 1 DA: '"data" means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording […]'.

[31] See, eg, art 2(1) GDPR.

[32] See, eg, art 8(1) CFR: 'Everyone has the right to the protection of personal data concerning him or her.'

[33] Art 4 no 1 GDPR.

[34] See also the breadth of the term 'personal data' ECJ, Judgment Case C-582/14 *Breyer* ECLI:EU:C:2016:779, [2016] § 32 ff; Judgment Case C-434/16 *Nowak* ECLI:EU:C:2017:994, [2017] Rn. 27 ff; Judgment Case C-579/21 J.M. ECLI:EU:C:2023:501, [2023] §§ 41 ff. *Cf* also the overly broad approach of the art 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136.

several activities involving a variety of parties, it can be quite difficult to decide under which conditions the person in question can be regarded as 'identifiable' in relation to which party. Many courts have struggled with the categorisation of IP addresses,[35] and the ECJ, in a recent illustrative decision, also with that of vehicle identification numbers.[36] The considerations already result in a very broad spectrum of data that can be linked to a person and then provide information about them.

Moreover, the identifiability of a person in a given situation or the much-discussed problem of re-identification are not the only issues. In light of its aims of protection and governance, data protection law does not only cover situations or activities in which a connection between data and particular persons actually exists or might be created by identifying steps. It also aims at preventing in advance legally undesirable connections between particular data and persons, the resulting knowledge about a person, and its potential disadvantageous use. Hence, it has to be more or less future-orientated and applicable prior to risks that have become manifest. The specification of personal data and the question of whether a person is identifiable therefore involve not only a substantive dimension, which may eventually be relational with respect to different parties, but also a temporal dimension. The possibility of referring data to persons over time and in contexts not yet foreseeable – data generated anew as personal data at a later point in time – must be considered to a certain extent. Under the conditions of a data-driven society and economy, data is constantly linked to persons in new and unpredictable ways. However, it cannot be sufficient for activating protection that somebody might link data to a person somehow at some point in time. Otherwise all data would have to be classified as personal data. Data protection law would be overinclusive and end up being a 'law of everything'.[37]

From these difficulties associated with the description and delimitation of personal data, we can draw several conclusions. Beyond pure identification data, the answer to the question of which data relates to a person requires a description of the quality that the relationship between the data and the person concerned must have, as well as a description of the contexts in which the handling of data and information takes place. In both respects, evaluative judgements and assumptions of probability come into play. To a considerable extent, prognoses and typifications may enter the picture. The personal-relatedness of data is rarely determined by looking at a single piece of data separately but rather with a view to the information and the knowledge that can be produced, to the overarching context, under certain circumstances to different relationships and participants, and through evaluative decisions.

The answers to the question of when data is personal are just as legally constructed as the concept of data. The understanding and delimitation of 'personal data' must be conceptualised against the background of the protected interests, which are the reason for data protection. Thus, it is not a seemingly easily detectable personal-relatedness of data as such that justifies the protection of data subjects. It is *the other*

[35] See, eg, the judgment of the Canadian Supreme Court, *R v Bykovets*, (2024) SCC 6, which is controversial concerning how to determine the information content of IP addresses.

[36] ECJ, Judgment Case C-319/22 *Gesamtverband Autoteile-Handel e. V.* ECLI:EU:C:2023:385, [2023] § 44 ff.

[37] N Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 *Law, Innovation, and Technology* 40.

way around: the reasons for protection make it possible to determine the personal-relatedness of data. Hence, the necessity of substantiating data protection interests – in more depth than a mere remark about a personal-relatedness of data – does not vanish. Such an approach is not only normatively convincing. It enables us, for example, to find solutions for scenarios that occur more frequently with the Internet of Things: data refers to several people in different ways, so that legal positions must be justified in more detail.

iii. Understanding 'Personal Data' within a Network of Basic Elements

At this point, it has already become clear that, from a constitutional and legal perspective, data protection deals with a highly complex subject matter. It is not about data as such. We must expand this isolated view by including further elements, in particular at a basic level the element of information, in the structural dimension knowledge, in the temporal dimension the flow of data and information, and in the broader context decisions, actions, and their consequences. Data protection aims at regulating data processing and data architectures but also at regulating the production of information and knowledge, at influencing the decisions based on such knowledge, and at preventing adverse consequences for the individuals affected.

It is of utmost importance for the understanding of data protection law that data and information must not be seen as if they were synonymous.[38] If their differentiation is considered to be irrelevant, neither the characteristics of data protection law nor the challenges it faces can be worked out. This is true even though legal definitions and some scholarly contributions might not reflect this in the required manner.

Data protection law addresses data, on the one hand, as an *objectified entity* that is characterised by a *specific technology-dependent materiality*. Data might be described as characters, symbols, or binary digital units that are stored in a certain format on a data carrier, including written documents or videos as well as data digitally stored on hard drives or mobile data storage devices. On the other hand, data protection law addresses data – and more precisely: personal data – because it can acquire informational significance in social contexts. Data is relevant as 'potential information'. This is to be understood more or less abstractly; as we have seen, it does not mean that there are fixed intrinsic meanings associated with the data. Furthermore, data can be decoupled from its potential informational significance to a certain extent; it can be identified as a distinct entity and become the subject of law even if it contributes to information and knowledge only in conjunction with other data or processing procedures. Data is often less important as a single piece of data but rather as part of data processing or data architectures. Without any potential informational significance, however, the legal relevance required in the context of data protection law is lacking.

In contrast to data, pieces of information are *elements of meaning* that may be based on data (or on observations or communications) and are then created by

[38] More closely Albers (n 9) 87 ff.

interpretations which take place in a particular social context.[39] Information is context-dependent in an elementary way. Although this insight may be well-established today, people hardly face up to the difficulties this entails for legal regulation. In the structural dimension of such context, *knowledge* – founded upon texts, files, archives, registers, databases, or expert systems, but also upon institutional, organisational or procedural arrangements – makes interpretation possible and limits the possibilities of interpretation.[40] In the temporal dimension, data as well as information is constantly generated anew and altered during *processing operations* or *flows of data and information*. Information and knowledge are increasingly recognised and worked out as distinct topics of law. They are also crucial factors in decision-making; they serve as bases for certain decisions and actions. Such decisions have consequences and may have an adverse effect on the person to whom the data and information refer. If disadvantages are normatively undesirable and unjustified, protection against such disadvantages – or even against the mere risk of such disadvantages arising – is one of the reasons for data protection. There are other reasons that can be elaborated on in the determination of protected interests. At this point, it should only be made clear that understanding data protection requires thinking in social relations, in overarching contexts and in processes. The scope and form of considering social contexts depend on how relatively loose or condensed the relationship between data and knowledge and actions and decisions is in the focused context.

As a result, data must be conceived of within a network of several basic elements. It is one, but not the only reference point. At the same time, these analyses have shown at what fundamental level we are working when regulating data and information.[41] It is as fundamental as regulating decisions or actions.

III. Familiar, but Fuzzy and Manifold Foundations of Data Protection Interests

Now that we have arrived at regulation, the next section analyses the familiar, but fuzzy foundations of data protection interests that are acknowledged at a constitutional level. How data protection interests are identified and described depends, of course, on the legal system and legal culture of the country concerned, on what is enshrined in the Constitution, or on the relationship between the legislature and the courts. Last but not least, constitutional concepts are always characterised by an interplay of substantive as

[39] Data and information are above all not synonyms because, although data as a basis for information may provide information, it presupposes far more than just data. Information cannot be described without observing knowledge structures, processes and the broader social context in which it arises.

[40] In more detail and with further references M Albers, 'Umgang mit personenbezogenen Informationen und Daten' in A Voßkuhle, M Eifert and C Möllers (eds), *Grundlagen des Verwaltungsrechts* vol I, 3rd edn (Munich, Beck, 2022) § 22 Rn 8 ff.

[41] These considerations also imply that it is always necessary to think through, in the context of the relevant norms, what normative role the terms 'data' or 'information' play and what exactly is therefore meant by them. *Cf* D Hallinan and R Gellert, 'The Concept of "Information": An Invisible Problem in the GDPR' (2020) 17(2) *SCRIPTed* 269 ff.

well as doctrinal and methodological considerations. Nevertheless, raising awareness of achievements and shortcomings of approaches can be fruitful.

Among the familiar foundations of data protection interests are the right to privacy, the right to informational self-determination, and the right to the protection of personal data. Rights to privacy are the bedrocks of broad debates and judicial decisions in the US as well as in some other countries, such as Canada, India, or South Africa. The understanding of the scope of protection of article 8 ECHR, the right to respect for private life, home, and correspondence, has been gradually extended to include data protection interests. The right to informational self-determination is a German peculiarity, but one that has attracted worldwide attention. The European Charter of Fundamental Rights – as a more recent codification that endeavours to meet the needs of modern society – guarantees everyone the right to the protection of personal data concerning him or her. The following sections analyse these legal foundations with a primary view to case law and aim at identifying achievements, weaknesses, and challenges. Our overview of case law begins with the US, a cradle of a 'right to privacy'.

A. Right to Privacy

i. Approaches and Developments in Case Law

To what extent 'privacy' is a suitable description of protected interests and how rights to 'privacy' must then be conceptualised in detail is part of a broad debate in the US. In reaction to media intrusions, the famous article by Warren and Brandeis in 1890 advocated the recognition of a right to privacy, shaped as a 'right to be let alone',[42] as part of tort law and thus put the idea on the map. While the term 'privacy' is not explicitly used in the text of the US Constitution, there are various approaches in the jurisdiction to anchor its more or less specified protection with regard to guarantees of primarily the First,[43] Fourth,[44] Fifth,[45] and Fourteenth[46] Amendments in a way that these guarantees have privacy as their underlying idea, and that this, in turn, lends itself to a methodologically broad interpretation of their subject matter and scope.[47]

[42] SD Warren and LD Brandeis, 'The Right to Privacy' (1890) 4/5 *Harvard Law Review* 193.

[43] 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.'

[44] 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

[45] 'No person shall […] be deprived of life, liberty, or property, without due process of law […].'

[46] '[…] nor shall any State deprive any person of life, liberty, or property, without due process of law […].'

[47] Methodologically partly with references to the Ninth Amendment: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.' See Justice Goldberg Concurring Opinion in *Griswold v Connecticut* 381 US 479, 489 ff (1965).

In several judgments of the US Supreme Court, these possible approaches have been worked out with regard to more closely specified individual decisions and relationships 'lying within the zone of privacy created by several fundamental constitutional guarantees […]'.[48] In the landmark judgment *Roe v Wade*, the Court held that 'a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution'.[49] This hereafter acknowledged 'right of personal privacy includes the interest in independence in making certain kinds of important decisions'.[50] Such decisional privacy is not assigned solely to liberty[51] because it is not about freedom of decision as such but about an even stronger protection for the 'most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy'.[52] The allocation of decision-making options is linked to certain spaces or topics and is inspired by the traditional differentiation between the individual's private matters and the spheres of decision and influence (also) open to others.

Privacy as a protected interest has been further outlined by interpreting the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures', established in the Fourth Amendment, and by specifying which spaces and objects are protected against what. The protection of the (relative) inviolability of the home as the spatial sphere of private life, which is delineated in terms of its functions as well as physical boundaries (for example, walls or fences), is a classic paradigm case. The protection of the secrecy of telecommunications can also be captured by using spatial metaphors, which address the network of communication relationships that are created via the use of certain communications technologies and services. Over time, the jurisdiction has moved away from restricting the protected good to 'material things – the person, the house, his papers, or his effects […]'[53] characterised by corporeal, material, or physical features and boundaries and regularly existing possibilities of control. Likewise, the understanding of what 'searches and seizures' are has been dissociated from the notion that an 'entry of the houses'[54] would be required for the approval of a relevant encroachment. In response to changes in the way society communicates, the US Supreme

[48] 381 US 479, 485.

[49] *Roe v Wade*, 410 U.S. 113, 152 (1973), and the Court stated in the following (at 153) that this 'right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.' Recently, this decision has been overruled by the US Supreme Court's judgment *Dobbs v Jackson Women's Health Organization*, 597 U.S. 215 (2022), with as yet not fully foreseeable ramifications.

[50] *Whalen v Roe*, 429 U.S. 589, 599 f (1977); *Carey v Population Services International*, 431 U.S. 678, 684 (1977).

[51] See, however, the sophisticated argumentation with some well-justified criticism of J Bellin, 'Pure Privacy' (2021) 116 *Northwestern University Law Review* 463, 477 ff, 481 ff.

[52] *Planned Parenthood of Southeastern Pa. v Casey*, 505 U.S. 833, 851 (1992).

[53] In *Olmstead v United States* 277 U.S. 438 (1928), the question before the Court was whether the use of evidence of private telephone conversations, intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments. In a 5:4 decision, it was held that there was no violation of the Fourth and Fifth Amendments. Chief Justice Taft wrote the majority judgment, holding that (at 464): 'The Amendment itself shows that the search is to be of material things – the person, the house, his papers, or his effects …'.

[54] See for the 'trespass doctrine' *Olmstead v United States*, 277 U.S. 438, 464 (1928). See also the dissent of Justice Brandeis in this respect.

Court reached the landmark decision '*Katz v United States*':[55] An enclosed public telephone booth is an area where a person has a constitutionally protected reasonable expectation of privacy, and eavesdropping activities of governmental agencies constitute a 'search and seizure' within the meaning of the Fourth Amendment that extends as well to the recording of oral statements.

For the subsequent case law, profound rearrangements, abstractions, and novel key concepts are crucial, especially the argumentation that 'the Fourth Amendment protects people, not places',[56] along with the 'reasonable expectation of privacy' test,[57] which places the emphasis on social relationships as well as on the boundaries that arise through them, and the extended understanding of encroachments. Substantive approaches based on traditional images of the safeguarded person or house are supplemented by functional approaches: the protective function is the guarantee of privacy, and what fulfils the functions of such privacy under the given social conditions, based on expectations of privacy that society acknowledges as reasonable, should be safeguarded. On the one hand, this leads to flexibility, but on the other hand, to a loss of legal certainty. This is because descriptions of social contexts and functional relations depend on the predefined theoretical framework and theoretical assumptions, for example, a theory of the individual and individuality.[58] The extension of the scope of protection goes hand in hand with an expanded understanding of 'search and seizures'. To a certain extent, the permissibility of these encroachments has always indicated that fundamental rights can include a protection against data collection; however, their traditional understanding was linked to certain activities against which a high level of protection is explainable due to the intrusiveness of the methods or the risks of their use regarding protected interests.[59] A more abstract understanding of search and seizures makes it possible to include new activities and methods made possible by technological developments as well as further encroachments of an informational nature. In turn, this leads to a loss of criteria that limit the spectrum of encroachments covered and of legal certainty. The subsequent case law illustrates the adaptability to social and technical developments as well as constant discussions regarding both the underlying legal approaches and the subsumption of the specific circumstances of the cases.[60]

[55] *Katz v United States*, 389 U.S. 347 (1967). Charles Katz was a gambler who used a public telephone booth to transmit illegal wagers. Unbeknownst to Katz, the FBI, which was investigating Katz's activity, was recording his conversations via an electronic eavesdropping device attached to the exterior of the phone booth. Subsequently, Katz was convicted based on these recordings. He challenged his conviction, arguing that the recordings were obtained in violation of his Fourth Amendment rights.

[56] *Katz v United States*, 389 U.S. 347, 351 (1967).

[57] In the following, the 'reasonable expectation of privacy' has become a pivotal pattern of argumentation and been relied on by various other jurisdictions while developing the right to privacy.

[58] *Cf* Gavison (n 6) 445.

[59] *Cf* also the dissent of Justice Alito, joined by Justice Thomas, *Carpenter v United States*, 585 U.S.____ (2018), 10 f.

[60] For example, whether 'reasonable expectations of privacy' can be recognised, is addressed in *United States v Miller*, 425 U.S. 435 (1976), in *Minnesota v Olson*, 495 U.S. 91 (1990), or in *Minnesota v Carter*, 525 U.S. 83 (1998). Whether there is a 'search' under the Fourth Amendment, is discussed with regard to an installation and use of a pen register in *Smith v Maryland*, 442 U.S. 735 (1979), to the thermal imaging of the house in *Kyllo v United States*, 533 U.S. 27 (2001), or to a GPS tracking device on a vehicle in *United States v Jones*, 565 U.S. 400 (2012). See also *Riley v California*, 573 U.S. 373 (2014), for the search and seizure of digital contents of a cell phone.

This becomes particularly evident in *Carpenter v United States*.[61] In this landmark ruling, the majority highlighted that the conception of the Amendment has been expanded 'to protect certain expectations of privacy', which could be positively assessed for cell site location information in light of their informative content and regardless of the fact that this data is held and retrieved by the wireless carrier.[62] The four dissents presented a variety of arguments, which spanned from fundamental criticism of the 'Katz' test[63] to the insistence on 'accepted property principles as the baseline for reasonable expectations of privacy'[64] up to the proposal to revisit the 'kind of legal interest' that 'is sufficient to make something *yours*' and 'the source of law that determines that' in order to also give room for legislative participation.[65]

Beyond the Fourth Amendment, the informational dimension of the right to privacy is addressed to a certain extent by using the idea of a zone of privacy created by several fundamental constitutional guarantees. The judgment '*Whalen v Roe*' was the starting point for differentiating kinds of interests which are covered by this protection,[66] even though the grounds of this judgment were fluctuating when locating these interests within the Constitution.[67] Besides the interest in independence in making certain kinds of important decisions, the individual interest in avoiding disclosure of personal matters was identified.[68] In the following, the informational dimension of privacy was of broader relevance in '*NASA v Nelson*', a case that dealt with NASA's background checks of contract employees.[69] The majority judgment chose to assume that a privacy interest of constitutional significance was at stake, but considering the legal safeguards, it concluded that there was no violation.[70] This line of reasoning was sharply criticised by the concurring opinions.[71] Their findings instead were that there is no constitutional right to 'informational privacy'.

Despite the recognition of different kinds of interests in the case law of the US Supreme Court, 'privacy' offers only limited, mostly accessory informational protection. Although some of the decisions address digital devices or advanced surveillance methods,[72] there is little success in developing sophisticated concepts of the protection

[61] Timothy Carpenter was charged with several crimes after wireless carriers handed over the cell site location information generated by his phone to the FBI and these data supported the suspicion that he had been involved in these crimes, *Carpenter v United States*, 585 U.S. ____ (2018).

[62] *Carpenter v United States*, 585 U.S. ____ (2018), p 5; *cf* for the protection of 'a person's expectation of privacy in his physical location and movements' pp 7 ff and for the discussion of the former 'third-party doctrine' pp 9 ff.

[63] See the dissent of Justice Thomas in *Carpenter v United States*, 585 U.S. ____ (2018).

[64] Dissent of Justice Kennedy, joined by Justice Thomas and Justice Alito, *Carpenter v United States*, 585 U.S. ____ (2018) p 22.

[65] Dissent of Justice Gorsuch, *Carpenter v United States*, 585 U.S. ____ (2018), p 13.

[66] *Whalen v Roe*, 429 U.S. 589 (1977) dealt with obligations of health care providers to store the private information of patients who received prescriptions for drugs.

[67] C Shachar and C Zubrzycki, 'Informational Privacy After *Dobbs* (2023) 75 *Alabama Law Review* 1, 12 ff.

[68] *Whalen v Roe*, 429 U.S. 589 (1977), at 598 f. See also with partly different considerations, *Nixon v Administrator of General Services*, 433 U.S. 425(1977) at 457.

[69] *NASA v Nelson*, 562 U.S. 134 (2011).

[70] Many questions remain unclear in the grounds, *cf* CP Moniodis, 'Moving from Nixon to NASA: Privacy's second strand – A right to informational privacy' (2012) 15 *Yale Journal of Law & Technology* 139, 157 ff.

[71] Concurring opinion of Justice Scalia, joined by Justice Thomas.

[72] See, eg, the reasoning in *United States v Jones*, 565 U.S. 400 (2012), in *Riley v California*, 573 U.S. 373 (2014), and in *Carpenter v United States*, 585 U.S. ____ (2018).

that is constitutionally guaranteed. As the grounds of the recent judgment '*Dobbs v Jackson Women Health Organization*' may illustrate,[73] the reasons for this have to do with the limits of the legal anchors and the methodological strategies. Catchphrases such as 'dignity versus liberty'[74] cannot capture the entire background and would be an exaggeration.

A more elaborated development of a constitutional right to privacy can be found in the case law of the Canadian Supreme Court. This is true, although the guarantees this Court refers to – most notably Section 8 and also Section 7 of the Canadian Charter of Rights and Freedoms[75] – are quite similar to those in the US. The understanding of the Charter as a 'purposive document'[76] whose spirit 'must not be constrained by narrow legalistic classifications based on notions of property'[77] leads to an abstract and broad understanding of Section 8 in the sense of a 'right to privacy'[78] that is shaped by the 'underlying values of dignity, integrity and autonomy'.[79] The pattern of 'reasonable expectations of privacy' has been essential for this understanding[80] and normatively assessed with a view to the 'totality of circumstances'.[81] The approach is sufficiently flexible to allow a distinction to be made between 'types of privacy interests – territorial, personal, and informational'.[82] Informational privacy interests are then described primarily as interests in the confidentiality, non-disclosure, non-dissemination or individual control of information, especially but not only in the case of intimate details on the individual's lifestyle and personal choices.[83] Recent judgments go further, differentiating privacy as secrecy, as control and as anonymity,[84] and pointing to 'informational self-determination'.[85] Some cases give rise to the development of more specific considerations which reflect the characteristics of information.

[73] *Dobbs v Jackson Women Health Organization*, 597 U.S. 215 (2022). The majority judgment emphasises that the reasons for overruling *Roe v Wade* and *Planned Parenthood v Casey* are partly of substantial nature, but above all, it is the methodological approach that is being subjected to a fundamental criticism, with as yet not all impacts predictable. For the discussion see, eg, S Kamin, 'Katz and Dobbs: Imagining the Fourth Amendment Without a Right to Privacy' (2022) 101 *Texas Law Review Online* 80.

[74] *Cf* JQ Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' (2004) 113 *Yale Law Journal* 1151.

[75] Section 8 states: 'Everyone has the right to be secure against unreasonable search or seizure.' Section 7 guarantees that 'Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.'

[76] See the methodological considerations in *Hunter et al v Southam Inc.*, [1984] 2 S.C.R. 145, 155 ff, 156 (for the citation).

[77] *R. v Dyment*, [1988] 2 S.C.R. 417, at 15.

[78] See as a landmark decision *Hunter et al. v Southam Inc.*, [1984] 2 S.C.R. 145, 155 ff.

[79] *R. v Plant*, [1993] 3 S.C.R. 281.

[80] *Hunter et al. v Southam Inc.*, [1984] 2 S.C.R. 145, 155 ff; *R. v Dyment*, [1988] 2 S.C.R. 417, at 15; *R. v Plant*, [1993] 3 S.C.R. 281.

[81] *R. v Tessling*, 2004 SCC 67, at 31 ff.

[82] *R. v Spencer*, 2014 SCC 43, at 35; see also *R. v Dyment*, [1988] 2 S.C.R. 417, at 19 ff; *R. v Tessling*, 2004 SCC 67, at 20 ff.

[83] *R. v Dyment*, [1988] 2 S.C.R. 417, at 31 ff.

[84] *R. v Spencer*, 2014 SCC 43, at 38.

[85] *R. v Jones* 2017 SCC 60, at 39, quoting *R. v Dyment* and the report of the Task Force, Privacy and Computers, 1972, 13, 'all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit'. See also *R. v Bykovets*, 2024 SCC 6, at 32. See further *R. v Tessling*, 2004 SCC 67, at 23, quoting Westin (n 11) 7: 'the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others'. *Cf* for the jurisdiction of the German FCC section III.B of this chapter.

The landmark decision '*R. v Dyment*' notes that if 'the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated'.[86] It also highlights that 'situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected',[87] implying a pivotal role of purpose specification and purpose limitation in the processing of data and information. Cases on the Internet have led to a further differentiation of informational privacy in interests such as secrecy, control, or anonymity. The recent judgment '*R. v Bykovets*' underlines that the subject matter of the protection revolves around information, not just data, and the dispute between majority opinion and dissents centres on the problem of determining the information content of IP addresses.[88] Nevertheless, the informational protection is repeatedly referred back to the underlying, albeit highly abstractly interpreted, 'protection against unreasonable search and seizure'. All in all, specific patterns and limitations shape the 'right to privacy' derived from Section 8 of the Canadian Charter of Rights and Freedoms, even if the Canadian Supreme Court goes considerably further in developing informational protection as compared to the US Supreme Court.

The recognition of a constitutional right to privacy in the jurisprudence of the Supreme Court of India also provides some insight. The text of the Constitution of India does not explicitly mention 'privacy'. Nevertheless, following an open methodological approach, including 'borrowing', the Supreme Court has derived a multi-layered and multi-dimensional right to privacy in its comprehensive '*Puttaswamy-I*-verdict' and reaffirmed this recognition in the '*Puttaswamy-II* case'.[89] Both judgments dealt with the constitutionality of the Aadhaar project, a centralised nationwide identification system based on biometric technology. The Court highlights that privacy 'constitutes the foundation of all liberty' and 'lies across the spectrum of protected freedoms'.[90] In its conclusions, it anchors the right to privacy on a broad foundation:

> [p]rivacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in art 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognized and guaranteed by the fundamental rights contained in Part III.[91]

[86] *R. v Dyment*, [1988] 2 S.C.R. 417, at 23: 'This is inherent in the notion of being *secure* against unreasonable searches and seizures.'

[87] *R. v Dyment*, [1988] 2 S.C.R. 417, at 22, 29 ff. In this case, the appellant had a traffic accident. A doctor collected a vial of free-flowing blood for medical purposes without the appellant's knowledge or consent. Later on, he handed the blood sample over to a police officer. The appellant was subsequently charged and convicted of impaired driving.

[88] *R. v Bykovets*, 2024 SCC 6.

[89] *Justice KS. Puttaswamy (Retd) v Union of India*, Judgment on 24 August 2017, Writ Petition (Civil) No 494 of 2012; (2017) 10 SCC 1; AIR 2017 SC 4161; and *Justice KS. Puttaswamy (Retd) v Union of India*, Judgment on 26 September 2018, AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1. While the right to privacy is recognised as a fundamental right in the *Puttaswamy-I*-decision, the Aadhar scheme has nevertheless been held constitutional in *Puttaswamy-II*.

[90] *Puttaswamy-I*, Part R (243, 244; Chandrachud J).

[91] *Puttaswamy-I*, Part T (266; Chandrachud J). Already in earlier case law, the right to life enshrined in art 21 of the Constitution has been interpreted as a basic right to a decent existence and has been given an expansive scope. *Cf* also regarding the jurisdiction of the Supreme Court of Pakistan S Aftab, *Comparative Perspectives on the Right to Privacy* (Dordrecht, Springer, 2024) 99 ff.

Different strands are covered, among others, informational privacy.[92] It is in line with the multi-layered and broad approach that the right to privacy is not only conceptualised as a right of defence against encroachments. It also includes duties of the state and mandates it to 'put in place a positive regime'.[93] Since the Aadhaar project raises many questions that are genuine data protection issues beyond common notions of privacy, it is particularly interesting that the Court, after addressing the characteristics of data and information, notes that 'apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual […] and the principle of non-discrimination'.[94]

What shape does a right to privacy take when it is explicitly enshrined in constitutional codifications? Textually and systematically, the protection under the right to privacy is usually placed in more traditional contexts of home, correspondence, or property, as well as search and seizures. An example of this is Section 14 of the Bill of Rights in the Constitution of the Republic of South Africa, 1996.[95] However, the anchoring of the right to privacy in the form of a general term – in conjunction with doctrinal and methodological considerations – allows the Constitutional Court of South Africa to develop this right relatively independently. The Court underlines the interrelationships between privacy, dignity, autonomy, and equality, as well as, in some cases, other freedom rights that are also affected, for example, the rights to freedom of expression and the media.[96] Nevertheless, 'privacy' implies certain patterns of thought, such as the juxtaposition of privacy and publicity, the differentiation of more or less personal realms, or the emphasis on an individual right to decide on disclosure. To a certain extent, such thought patterns are also at work when it comes to the issues of data protection.[97]

Article 8 of the European Convention on Human Rights (ECHR) expressly provides for the right of everyone to respect for his or her private life and correspondence.[98] Since the European Court of Human Rights (ECtHR) sees itself as the pivotal European court in the field of international law and as part of a network between the signatory states and the European courts within which these courts and their

[92] See *Puttaswamy-I*, Part S (246 ff; Chandrachud J).

[93] *Puttaswamy-II*, Part G (232; Chandrachud J, dissenting); *cf* also *Puttaswamy-I*, Part S (p 254; Chandrachud J).

[94] *Puttaswamy-I*, Part S (246 ff, 252; Chandrachud J).

[95] Section 14 of the Bill of Rights provides that everyone has the right to privacy, which includes the right not to have: (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed.

[96] *Cf Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 112 ff.

[97] *Cf* the judgments *Bernstein and Others v Bester NO and Others* (CCT 23/95) [1996] ZACC 2, at 56 ff; *NM and Others v Smith and Others* (CCT 69/05) [2007] ZACC 6, at 32 ff; *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 23 ff.

[98] 'Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

decisions increasingly interact,[99] it has moved away from the traditional understanding of the ECHR in terms of international minimum standards. According to its case law, article 8 ECHR protects a broad spectrum of interests.[100] Besides the protection of personal activities, decisions or spatial areas, which always included social relationships and public activities to a certain extent, protection was gradually developed with regard to the handling of personal information and data. The initial judgments dealt with traditional cases of phone surveillance and, thus, the right to respect for correspondence. In such cases, first guidelines were developed, for example, that business connections are covered by protection if reasonable expectations of privacy protection can be recognised, or that an impairment does not depend on whether and to what extent recordings are subsequently used or whether concrete disadvantages have arisen – an argumentation pattern that has always existed in cases of telecommunications surveillance as a typifying approach. The informational protection of the right to respect for the 'private life' was to some extent based on these initial guidelines, not least because the data processing steps that followed the interception were subsumed under this right.[101] The protection extends to data that originates within a private sphere. To a certain extent, it can also cover data that is publicly accessible, for example, in the event of systematic collection and storage by public authorities, or in the case of a compilation, use, or other form of processing of personal data that the data subject would not reasonably expect. In the subsequent case law, the focus has increasingly shifted from the private sphere as the source of the data to its informational content. A wide range of data has been classified as belonging to private life, such as tax data, medical data and information, data on the health or sexual life of somebody, personal data revealing political opinions, such as information about participation in peaceful protests, the IP address or geolocation data insofar as it can be related to individuals, a person's image and biometric data, but also photos and video recordings or DNA samples as data carriers.[102] Data processing steps are differentiated and, if necessary, independently assessed as an intrusion.[103] In principle, the Court upholds the presumption that the collection, recording, use, or publication of private life can constitute an impairment, regardless of whether the

[99] M Albers 'Höchstrichterliche Rechtsfindung und Auslegung gerichtlicher Entscheidungen' in G Lienbacher, B Grzeszick and C Calliess et al (eds), *Grundsatzfragen der Rechtsetzung und Rechtsfindung*, VVDStRL vol 71 (Berlin, de Gruyter, 2012) 257 (272 ff, 287 ff).

[100] For a comprehensive overview of the case law see ECtHR, Guide on art 8 of the European Convention on Human Rights, right to respect for private and family life, home and correspondence (last update: 5.11.2024), www.ks.echr.coe.int/web/echr-ks/article-8-all-updates; ECtHR, Factsheet – Personal data protection (last update: February 2024), www.echr.coe.int/documents/d/echr/fs_data_eng.

[101] *Cf* ECtHR, No 27798/95 *Amann* ECLI:CE:ECHR:2000:0216, [2000] §§ 44 ff, 64 ff.

[102] *Cf*, ECtHR Case No 20383/04 *Khmel* ECLI:CE:ECHR:2013:1212, [2013] §§ 41 ff, 49; Case No 931/13 *Satakunnan* ECLI:CE:ECHR:2017:0627, [2017] §§ 133 ff; No 66490/09 *Mockutė* ECLI:CE:ECHR:2018:0227, [2018] §§ 93 f; No 62357/14 *Benedik* ECLI:CE:ECHR:2018:0424, [2018] §§ 100 ff, 107 ff; No 50001/12 *Breyer* ECLI:CE:ECHR:2020:0130, [2020] §§ 76 ff; No 75229/10 *Dragan Petrović* ECLI:CE:ECHR:2020:0414, [2020] §§ 69, 79; Nos 3153/16 and 27758/18 *Drelon* ECLI:CE:ECHR:2022:0908, [2022] §§ 79 ff; No 11519/20 *Glukhin* ECLI:CE:ECHR:2023:0704, [2023] §§ 64 ff.

[103] ECtHR, No 20383/04 *Khmel* ECLI:CE:ECHR:2013:1212, [2013] §§ 40 ff; No 42788/06 *Surikov* ECLI:CE:ECHR:2017:0126, [2017] §§ 75, 84 ff; No 931/13 §§ 134 ff.

data is sensitive or whether the data subject has suffered specific disadvantages.[104] However, potentially detrimental consequences do play a role in the overall assessment of protection.[105] When such effects are taken into account, other freedoms may become relevant as well, for example, the freedom of expression.[106]

The ECtHR specifies more detailed requirements for the necessary legal basis in a very differentiated manner, depending on the context and dimension of protection, while recognising the more or less far-reaching margin of appreciation of the signatory states. For example, state surveillance measures, especially if they are secret at certain stages, require a series of coordinated minimum legal precautions.[107] And the state does not adequately fulfil its duty to protect unless it ensures respect for private life among private individuals by creating a legal framework that takes account of the different protection interests in a particular context.[108] article 8 ECHR can also provide (limited) rights of knowledge, such as the right to information or access to files with regard to personal data or documents held by the authorities.[109]

ii. Achievements and Shortcomings of Privacy as Protected Interest

Irrespective of whether the constitutional protection of (respect for) privacy is explicitly enshrined or derived from other fundamental rights, its long and rich tradition as an idea makes it easier to address it as a subject matter of fundamental rights protection at different levels and in different contexts. The heterogeneous framings and the shifting meanings of privacy also make it easier to refer to seemingly established views, just as they are often the reason for talking past one another. How constitutional provisions are interpreted in terms of a 'right to privacy' depends, of course, on the legal system and culture, as well as on the role and self-understanding of the courts, and not only on substantive but also on doctrinal and methodological considerations. Nevertheless, some achievements and weaknesses of privacy as a protected interest when it comes to constitutionalising data protection can be identified, which emerge as issues across jurisdictions.

In terms of content, it is a particular achievement that the right to (respect for) privacy can be applied to very different and wide-ranging subject matters of protection.[110]

[104] ECtHR, No 28 341/95 *Rotaru* ECLI:CE:ECHR:2000:0504, [2000] §§ 42 ff; No 44 647/98 *Peck* ECLI:CE:ECHR:2003:0128, [2003] §§ 57 ff; No 62 332/00 *Segerstedt-Wiberg* ECLI:CE:ECHR:2006:0606, [2006] §§ 69 ff; No 30 562/04 *S. and Marper* ECLI:CE:ECHR:2008:1204, [2008] §§ 58 ff; No 11519/20, 67 ff. See also for a legal obligation of Telegram to decrypt Internet communications if they are encrypted No 33696/19 *Podchasov* ECLI:CE:ECHR:2024:0213, [2024] § 58.

[105] ECtHR, No 931/13, § 137; No 50001/12, §§ 74 ff; No 11519/20, §§ 65 ff; No 33696/19, § 51 ff.

[106] See ECtHR, Nos 58170/13, 62322/14 and 24960/15 *Big Brother Watch* ECLI:CE:ECHR:2018:0913, [2021] §§ 442 ff.

[107] ECtHR, No 47143/06 *Zakharov* ECLI:CE:ECHR:2015:1204, [2015] §§ 228 ff, Nos 58170/13, 62322/14 and 24960/15, §§ 322 ff; No 70078/12 *Ekimdzhiev* ECLI:CE:ECHR:2022:0111, [2022] §§ 291 ff; No 33696/19, §§ 63 ff.

[108] *Cf* ECtHR, No 61496/08 *Bărbulescu* ECLI:CE:ECHR:2017:0905, [2017] §§ 115, 120 ff.

[109] *Cf* ECtHR, No 10 454/83 *Gaskin* ECLI:CE:ECHR:1989:0707, [1989] § 37; No 62 332/00, §§ 99 ff; No 12 504/09 *Yonchev* ECLI:CE:ECHR:2017:1207, [2017] §§ 46 ff.

[110] *Cf* D Solove, *Understanding Privacy* (Cambridge (MA), Harvard University Press, 2008) 45: 'umbrella term'. *Cf* also more closely BJ Koops, B Newell, T Timan, I Skorvanek, T Chokrevski and M Galič, 'A Typology of Privacy' (2017) 38 *University of Pennsylvania Journal of International Law*, 483, 491 ff; Aftab (n 91) 39 ff.

On the one hand, this is due to its level of abstraction. In line with the basic dichotomies that have shaped the traditional understanding of privacy, some lines of reasoning take a very fundamental approach by emphasising that privacy is a crucial value for a liberal society and, in the sense of a precondition, essential for the exercise of other freedoms.[111] On the other hand, the concept of a private 'sphere' can cover different facets of protection, for example, personal decisions, particular spatial areas, and also the content of conversations or data that arise in or can be attributed to that private sphere. As we have seen: 'Privacy' assigns something to a person or a group of people as their own concern and sets limits on others' access to it. The attribution already made in the concept – in particular, of data to the individual[112] – reduces the burden of giving reasons for protection needs. Just as the protected interests do not have to be specified in detail, it is not necessary to specify impairments and to break down precisely to what extent the person in question is actually exposed to disadvantages. As we have seen, the ECtHR even emphasises that an impairment does not depend on whether concrete disadvantages have arisen. The data subject as a fundamental rights holder has a protected negative-liberty status based on the principle of non-interference in the private sphere, which can be applied to various forms of intrusions, including the acquisition of data, information, and knowledge about the right-holder. Such an approach does not need to be more closely aligned with the characteristics of this particular subject matter to which the protection is extended. Provided that more detailed aspects of protection or of impairments are addressed, particularly in the balancing of interests, interdependencies between data protection and freedoms of decisions or behaviour that might be protected by specific fundamental rights show up.[113] In this sense, the right to privacy always points beyond itself.

Following traditional patterns for the development and justification of data protection has its disadvantages as well. Insofar as some courts, due to their doctrinal and methodological approach, are rather reluctant to make more extensive interpretations, the protection with regard to the handling of data and information is understood as an extension and more or less accessory to traditionally protected freedoms or at best one facet of protection among others. It is not explicitly information- and data-orientated but rather based on the assumption that data shares the privacy of the personal sphere from which they originate. Consequently, it is more or less designed as a sphere-related 'defence formula'. Difficulties arise already if data acquires an informational content that calls for protection only in the context of its further processing or use, for example, through the linking of data or additional knowledge. The paradigm of a private sphere directs attention primarily to the collection of data (as an intrusion into the personal

[111] See, eg, the Supreme Court of Canada, *R. v Dyment*, [1988] 2 S.C.R. 417, at 17 (quoting Westin, (n 11) 349 f): '[…] society has come to realize that privacy is at the heart of liberty in a modern state […] Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual.'; and the Supreme Court of India, *Puttaswamy-I*, Part R (243, 244).

[112] *Cf* the dissent of Justice Gorsuch, *Carpenter v United States*, 585 U.S. ____ (2018), 13, with the proposal to revisit the 'kind of legal interest' that 'is sufficient to make something *yours*'.

[113] For example: Constitutional Court of South Africa, *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 112 ff; ECtHR, Nos 58170/13, 62322/14 and 24960/15, §§ 442 ff.

sphere) and the requirements for its justification, for example, a search warrant. The subsequent data processing steps receive only limited attention and are not appropriately assessed in terms of their own potentially detrimental consequences. Insofar as other courts see their role as a proactive one and understand the relevant codification in the sense of a 'living constitution', they arrive at very sophisticated multi-layered and multi-dimensional conceptions, which also set a demanding task for the legislature. While the lines of reasoning are problem-orientated, they may be criticised for not being sufficiently grounded in the provisions, especially since the concept of privacy itself is under constant criticism.[114] In addition, to some extent, traditional patterns of thought still have an impact on the conceptions. The focus on 'privacy' runs the risk of failing to adequately develop the protected interests of data subjects and data protection law. References to informational self-determination, such as we find in some of the court decisions, are therefore not surprising.

At this point we can move on to the right of personality and the right to informational self-determination. In the jurisprudence of the German Federal Constitutional Court, this right has been developed not least in response to the weaknesses of the formerly recognised right to respect for privacy. It is tailored to the purpose of providing protection to the individual with regard to the handling of personal data and information.

B. Right to Personality and Informational Self-Determination

German law is famous for the development of a protected interest that has attracted worldwide attention: 'informational self-determination'. I would prefer to call it 'informational autonomy' because 'informational self-determination' is just a poor translation. However, this term is established, and therefore, I will stick to it.

i. Approaches and Developments in Case Law

The Federal Constitutional Court derived the 'right to informational self-determination' from article 2(1) in conjunction with article 1(1) of the Basic Law[115] in its decision concerning the census ('V*olkszählungsurteil*') taken in 1983.[116] The wording of these fundamental rights does not explicitly provide for a 'right to informational self-determination'. Instead, it refers to the protection of the free development of one's personality and to the inviolability of human dignity.

In our context, it is of particular interest that article 2(1) in conjunction with article 1(1) of the Basic Law has long been interpreted in the case law of the Federal Constitutional Court primarily as a 'right to respect for privacy'. Scholarly contributions

[114] See, eg, Bellin (n 51).

[115] Art 2 Basic Law: 'Everybody shall have the right to the free development of his or her personality […]'; art 1 Basic Law: 'Human dignity shall be inviolable. To respect and to protect it shall be the duty of all state authority.'

[116] Decisions of the FCC (BVerfGE) vol 65, 1. See also G Britz, ch 5 in this volume.

and an inspirational glance at American case law have contributed to the derivation of this right. In its early case law, the Federal Constitutional Court originally conceived of 'privacy' employing the spatial imagery of areas of retreat walled off from the outside world or situations for interaction and communication that are to remain, in principle, free of undesired inspection. Subsequently, issues were included that are typically classified as 'private' due to their information content. As a result, the right to respect for privacy has covered many constellations: the protection of medical files stored at the doctor's workplace from access by security authorities,[117] the use of secret tape recordings in a civil court proceeding,[118] the publishing of a fictitious interview about private matters in the press,[119] or a television movie about a murder in which the criminal, who has since been released, can be identified (the famous '*Lebach*-case').[120]

But then the '*Eppler*-case' resulted in a turning point.[121] In this case of an alleged public statement on a public matter, the FCC reached the conclusion that 'the right to respect for privacy' was not a suitable approach to grasp the problems of the case appropriately. Instead, the 'general right of personality' was derived from article 2(1) in conjunction with article 1(1) of the Basic Law.[122] This development is facilitated by the fact that the wording of article 2(1) of the Basic Law promises everyone the right to freely develop their personality. In the '*Eppler*-decision', the Court held that, in principle, individuals should be able to decide for themselves how they wish to present themselves to third parties or to the public, and whether and to what extent third parties may dispose of their personality.[123] Although the case was about statements falsely attributed to one's person, this description of the scope of protection has been understood as if the general right of personality provided a right that people see you the way you want to be seen. This paved the way for the right to informational self-determination.

According to the '*Census*-judgment', the right to informational self-determination confers on the individual the authority to, in principle, determine for themselves the disclosure and use of their personal data.[124] Individuals have the right to decide for themselves whether and how their personal data is to be revealed and used; in other words, they have a right to self-determination about the processing of data relating to them. An analysis of the broader background, previous case law, and academic debate can explain very well how the Federal Constitutional Court arrived at this subject

[117] BVerfGE 32, 373 [1972] – *Ärztliche Schweigepflicht (Medical Confidentiality)*; 44, 353 [1977] – *Durchsuchung Drogenberatungsstelle (Search of drug counseling center)*.

[118] BVerfGE, 34, 238 [1973] – *Tonband*.

[119] BVerfGE 34, 269 [1973] – *Soraya*.

[120] BVerfGE 35, 202 [1973] – *Lebach*.

[121] BVerfGE 54, 148 [1980] – *Eppler*. Erhard Eppler, a well-known member of the Social Democratic Party of Germany, was blamed for making a public statement on a public matter which he proved he had not made in this way and requested injunctive relief.

[122] BVerfGE 54, 148, 153 ff.

[123] BVerfGE 54, 148, 155.

[124] BVerfGE 65, 1, 43 [1983] – *Volkszählungsurteil*. Analysing the decision and its background Albers (n 9), 151 ff. Limitations to this broadly defined scope of protection – see Britz (n 116) – are considered by the court only when looking at the possibilities of restricting protection on the basis of the legal reservation, see BVerfGE 65, 1, 46 ff.

matter to be protected. The precursor of the right to informational self-determination, the right to respect for privacy, drew the same criticism in Germany as it did in the US-American privacy debate. The first point of criticism emphasised the relativity of the sphere of personal privacy: it could be described only in terms 'relative' to those receiving information.[125] Therefore, what was to be protected was not a predetermined sphere, but the capacity of the individual to decide to whom to disclose which information. Alan Westin formulated this idea in these terms as early as 1972.[126] The second point of criticism highlighted the fact that the need for protection was less about the private sphere as the context in which certain data emerges but rather about which information could be derived from data obtained and how that information could be used.[127] In other words, what is decisive is not the context the data originates from but rather the context in which the information is used. The Federal Constitutional Court responded to these central points of criticism by developing a right with a scope of protection which centres on individual decision capacities as well as on the context of use of personal data.[128] It also took up the acknowledged constitutionally protected goods of autonomy and freedom of decision and action, arguing as follows: free decision and action are possible only under certain circumstances. If people are unsure whether deviating behaviours may be stored as information and used to their disadvantage, they will try not to attract attention by such behaviour and will no longer be free to act at will.[129] That is why the protection of fundamental rights must cover the protection against information and data processing by the state. The Federal Constitutional Court concluded that, just as people can decide about their actions, they also have the right to determine how 'their' personal data will be processed. The protected persons also have the right to know by whom and for what purposes personal data referring to them are processed,[130] but that right is accessory in the context of the concept.

In the course of its case law, the FCC has long maintained a scope of protection defined in this way and, using it as a starting point, has developed a wide range of requirements with which statutory law must comply. These include the principles of purpose specification and purpose limitation, thresholds for the permissibility of data processing steps, and data security standards. Particular requirements can usually be traced back to the challenges raised by the case. The doctrinal reference point is often

[125] See B Schlink, 'Das Recht der informationellen Selbstbestimmung' (1986) 25 *Der Staat* 233, 242; D Solove, *The digital person* (New York and London, NYU Press, 2004) 212 f.

[126] AF Westin, *Privacy and Freedom,* 6 edn (New York, Atheneum, 1970) 42.

[127] See S Simitis, 'Chancen und Gefahren der elektronischen Datenverarbeitung' [1971] *Neue Juristische Wochenschrift (NJW)* 673, 680.

[128] For literary sources of the Court's decision see H Heußner (former judge at the BVerfG preparing the Census Decision), 'Das informationelle Selbstbestimmungsrecht in der Rechtsprechung des Bundesverfassungsgerichts' [1984] *Die Sozialgerichtsbarkeit (SGb)* 279, 280 f. Amongst others, the ideas of Westin have been received by the members of the Court, see E Benda (former President of the BVerfG participating at the Census Decision), 'Privatsphäre und "Persönlichkeitsprofil". Ein Beitrag zur Datenschutzdiskussion' in Leibholz, Faller, Mikat and Reis (eds), *Menschenwürde und freiheitliche Rechtsordnung* (Tübingen, Mohr Siebeck, 1974) 23, 32.

[129] BVerfGE 65, 1, 43.

[130] BVerfGE, 65, 1, 46.

the principle of proportionality, although it may not be the most appropriate reference point for some requirements.

In the aforementioned version of a right of individuals to decide whether and how 'their' personal data is to be disclosed and used, the right to informational self-determination was quite firmly established for a long time. But meanwhile, this version is in flux. It already has been modified to a certain extent. The FCC has thus reacted to scholarly criticism as well as to changes in its own case law on the right to respect for privacy and the general right of personality.[131] For instance, the Court clarified in its '*Caroline I*-judgment' that

> […] the general right of personality does not confer to the individual the right to be portrayed by others only as he or she views him- or herself or only as he or she wants to be perceived […] Such a broad protection would not only exceed the aim of protection, i.e. to avoid risks to the development of an individual's personality, but would also extend far into third parties' sphere of freedom.[132]

Thereby a pattern of argumentation has been abandoned that contributed to the definition of the scope of protection of the right to informational self-determination.[133] In relation to the state, the problem has arisen in cases such as electronic profiling and searches or automatic licence plate recognition that personal data is collected but quickly and automatically sorted out and deleted, raising the question of whether this is relevant to the scope of protection and may amount to an encroachment. In such cases, the Court has partially modified the protective functions and the scope of protection of the right to informational self-determination in a more or less well-thought-out manner.[134] In the '*Right to be Forgotten I*-judgment' of 2019, the Court has undertaken significant changes: Between private parties,[135] the right to informational self-determination provides the individual

> the possibility of influencing, in nuanced ways, the context and manner in which their data is accessible to and can be used by others, thus affording the individual considerable influence in deciding what information is available on them.[136]

Further elaboration of the right to informational self-determination continues to progress.

[131] For these changes see BVerfGE 97, 125, 146 ff [1998] – *Caroline I*; 97, 391, 403 ff; 101, 361, 382; 120, 180, 199.

[132] BVerfGE 101, 361–396 [1999] – *Caroline II*, para 70, www.bverfg.de/e/rs19991215_1bvr065396en.html.

[133] *Cf* M Albers, 'Grundrechtsschutz der Privatheit' [2010] *Deutsches Verwaltungsblatt (DVBl)* 1061, 1065 f.

[134] See BVerfGE 115, 320, 342 ff [2006] – *Rasterfahndung II*; 120, 378, 398 [2008] – *Automatisierte Kennzeichenerfassung*; 150, 244 [2018] – *Kennzeichenkontrolle Bayern* Rn 41 ff.

[135] The relationship between private parties is covered by fundamental rights via acknowledged third-party effects ('*Drittwirkung*'), however, an individual right to decide on the disclosure and use of personal data has always created substantial and doctrinal problems. See L Schertel Mendes, *Schutz vor Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung: Eine Analyse der Rechtmäßigkeit der Datenverarbeitung im Privatrecht* (Berlin, De Gruyter, 2015) 44 ff. *Cf* also for the doctrine of the '*Drittwirkung*' M Albers, 'L'effet horizontal des droits fondamentaux dans le cadre d'une conception à multi-niveaux' in Hochmann and Reinhardt (eds), *L'effet horizontal des droits fondamentaux* (Paris, Éditions Pedone, 2018) 177 ff.

[136] BVerfGE 152, 152–215 [2019] – *Recht auf Vergessen I*, Headnote 3 and Rn 83 ff, www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en.html.

ii. Achievements and Weaknesses of Informational Self-Determination as Protected Interest

The right to informational self-determination reaches far beyond the classical understanding of the right to respect for privacy. Its core element is a relatively abstract individual right to make decisions ranging from disclosure of data to their processing and to their use. This scope of protection is characterised by an approach that places the handling of personal data and information as such at the centre of attention. The protection provided is no longer derived from and no longer dependent on otherwise protected interests – such as 'privacy' – that have particular definitions and delimitations. It is an area in its own right. This opens up the possibility that the protection is being tailored appropriately to the subject matter. The protection directly aimed at the handling of personal data and information and the possible extension to a wide range of protection requirements that already exist or may arise in the future are an important step forward that the right to informational self-determination has brought.

Despite these achievements of the novel approach to protection requirements, there are shortcomings in the FCC's definition of the scope of protection. As explained, the approach opens up the possibility that the protection is being tailored appropriately to the subject matter. But this is precisely what the Court fails to do. The Court adheres to traditional patterns of thought with regard to both content and doctrine. In terms of content, the Court is guided by the familiar patterns used to describe freedom of decision and action, or property rights. After all, these patterns of free decision and action have been referred to in the argumentation of the census judgment's grounds in order to support the development of the right to informational self-determination. Additionally, even though the right to informational self-determination is derived from the right to the free development of personality and from human dignity, its scope of protection is to a certain extent shaped like a property right.[137] Similar to some US-American conceptions of privacy, informational self-determination is primarily thought of as a right of control over personal data.[138] Such an approach does not do justice to the distinct categoriality and characteristics of data, information and knowledge. It entails ontic ideas, as if data or even information were a kind of ball that can be held or passed on and that does not change in the process. It is no coincidence that the scope of protection of 'informational' self-determination relates to data, not information. The fact that others, be they government agencies or private individuals, are structurally involved with their own activities of interpreting, processing, and

[137] Sometimes it is emphasised that the BVerfG also stated: 'The individual does not have a right in the sense of an absolute, unlimitable mastery over "his/her" data; he/she is rather a personality that develops within a social community and is dependent upon communication', BVerfGE 65, 1, 43, 46. However, these grounds refer to the reservation allowing to limit the scope of protection by means of statutory rules. They do not alter the shaping of the scope of protection.

[138] The ideas of Westin (n 126) 42, which the BVerfG adopted, have also been cited in some rulings of the Canadian Supreme Court. See also C Fried, 'Privacy' (1968) 77 *Yale Law Journal* 475, 482, 483: 'Privacy […] is the *control* we have over information about ourselves […] is control over knowledge about oneself.' For more on these ideas and their critique, see A Allen, ch 1 in this volume.

creating constantly changing data and information is lost.[139] In its case law, the Court does occasionally address the informational content of data and the informational consequences in the social relations between the parties involved when it comes to discussing the impairment of the right to informational self-determination or to the balancing of interests required by the principle of proportionality.[140] However, as long as the scope of protection continues to be defined in its flawed conception, the Court's deliberations lack substantive and doctrinal consistency.

In terms of doctrine, the Court is guided by the familiar patterns of protection against encroachments. That means that the fundamental right's scope of protection is interpreted as safeguarding individual freedom (traditionally understood in a liberal way) against any impairments unless they are covered by statutory provisions which meet the principle of clarity and certainty, the principle of proportionality, and all other relevant constitutional requirements. This doctrinal approach results in specific forms of describing the subject matters or interests which are to be protected by fundamental rights as well as in specific functions and features regarding the statutory provisions. In particular, the idea is lost that an appropriate regulation of the handling of personal information and data must be multi-layered as well as manifold and requires a multitude of regulatory tools. Since the doctrinal approach leads to a limited perspective, the wide range of requirements that the Court has nevertheless developed in the course of its jurisprudence[141] is often not sufficiently linked to the scope of protection and can be better explained in terms of reasonable solutions to the challenges of the case. Relatively free-standing judicial findings raise problems not only of doctrinal consistency but also of the role and legitimacy of the courts. It simply does not work to comprehend a fundamental right's scope of protection merely in terms of its function to activate 'the fundamental need to justify […] data processing' or 'to create a starting point for a process that requires legal structuring with regard to the free development of personality'.[142]

The right to informational self-determination is quite popular in other countries' jurisdictions, as well as within the international scientific community. But we must be aware that the FCC, as I have mentioned above, has modified the scope of protection of this right in recent decisions. It has revised its approach only to a very limited extent in the state-citizen relationship, but more significantly in the relations between private individuals. The description of the scope of protection in these relations has been left rather vague, and the sharp distinction between the statements on the state-citizen relationships and those on the relations between private parties reveals an overly traditional understanding of the state. The interplay with the Charter of Fundamental Rights of the European Union, which is not only based on factual influences but is also doctrinally justified,[143] opens up opportunities for the necessary further development of fundamental rights.

[139] For a detailed analysis and critique, see Albers (n 9) 151 ff, 234 ff, 280 ff.
[140] This is emphasised by J Masing, ch 3 in this volume.
[141] See above III.B.i. and Masing (n 140).
[142] Masing (n 140).
[143] *Cf* Albers (n 99) 287 ff.

C. Right to the Protection of Personal Data

Aiming at being a modern charter covering contemporary challenges,[144] article 8(1) of the Charter of Fundamental Rights of the European Union (CFR) offers everyone a specific right to the protection of personal data concerning them.[145] Article 8(2) and (3) CFR point in part to the possibility of shaping or restricting the fundamental right via statutory regulations and in part contain guidelines for such regulations.[146] The explicit enshrinement of a right to the protection of personal data has been the model for the new similar anchor in article 5 LXXIX of the Constitution of the Federative Republic of Brazil.[147] Article 8(1) CFR stands alongside the protection of article 7(1) CFR, the right to respect for private and family life, home, and communications. Does that novel fundamental right advance the constitutional landscape and offer answers to the question of how to unfold the protected interests of data subjects?

i. Approaches and Developments in Case Law

In its initial decisions, the ECJ stated that article 8 CFR was 'closely linked' to article 7 CFR[148] and did not differentiate in more detail between the two fundamental rights.[149] Specific difficulties in distinguishing between the scope of protection of article 7 CFR on the one hand and article 8 CFR on the other arise for doctrinal reasons: article 52(3) CFR grants the rights of the Charter the same meaning and scope as the corresponding Convention rights, and article 7(1) CFR corresponds to article 8(1) ECHR, which is the foundation of data protection in the case law of the ECtHR. In its landmark '*Tele2 Sverige*-judgment', the ECJ does not address all the questions arising, but at least it explains that 'Art. 52(3) CFR does not preclude Union law from providing protection that is more extensive than the ECHR' and that

[144] See also F Picod, C Rizcallah and S Van Drooghenbroek (eds), *Charte des droits fondamentaux de l'Union européenne*, 3rd edn (Édition Bruylant, Bruxelles, 2023) art 8 Rn. 1.

[145] Art 8(1) CFR states: 'Everyone has the right to the protection of personal data concerning him or her.' The right to the protection of personal data concerning him or her is also anchored in art 16(1) TFEU. The difficulties in reconciling art 16(1) TFEU, arts 8, 52(1) and 52(2) CFR can be resolved by a teleological reduction of art 52(2) CFR. *Cf* ECJ (Grand Chamber) of 26 July 2017, Opinion 1/15, PNR, § 120.

[146] These sections read: '(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.'

[147] According to the amendment of this article in 2022, 'under the terms of the law, the right to protection of personal data is ensured, including in digital media'. See for the preceding development until the landmark ruling of the Brazilian Supreme Court on 7 May 2020, that paved the way for Congress to pass the constitutional amendment I Sarlet, 'The Protection of Personality in the Digital Environment' in Albers and Sarlet (n 1) 133 (137 ff).

[148] ECJ, Judgment (Grand Chamber) Case C-92, 93/09 *Schecke* ECLI:EU:C:2010:662, [2010] § 47.

[149] See ECJ, Judgment (Grand Chamber) Case C-92, 93/09, §§ 45 ff; Judgment (Grand Chamber) Case C-468, 469/10 *ASNEF/FECEMD* ECLI:EU:C:2011:777, [2011] §§ 41 ff. For more in-depth analyses of earlier case law P de Hert and S Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Gutwirth, Poullet, de Hert, de Terwagne and Nouwt (eds), *Reinventing Data Protection?* (Berlin, Springer, 2009) 3 (29 ff).

article 8 CFR 'concerns a fundamental right which is distinct from that enshrined in art 7 of the Charter and which has no equivalent in the ECHR'.[150]

However, the Court's interpretation of the scope of protection under article 8 CFR does not provide much substance. The '*Digital Rights Ireland*-judgment' indicates that article 7 CFR protects private life in a substantive sense, while article 8 CFR focuses on the processing of personal data in a way that is not limited to private life and sets its own requirements, for example, in terms of data security or in terms of protecting personal data against the risk of abuse and against any unlawful access and use.[151] The constituent elements of article 8(1) CFR are 'personal data' and their processing, irrespective of whether the information that can be obtained from the data is of a sensitive nature or whether any detrimental effects have been suffered.[152] Data processing phases are differentiated and assessed separately – not in isolation, however, but as relatively independent elements of a processing sequence.[153] In a closer context, the protected interests of data subjects are occasionally specified, such as the need for protection against comprehensive profiling or constant surveillance, against expectation-mediated constraints on actually protected behaviour, against the undermining of professional secrecy or informant protection, or against data misuse.[154] When developing these protected interests, the ECJ takes into account other fundamental rights of the European Charter as well as interests protected under secondary or national law.[155] This is quite convincing if we associate article 8 CFR with a bundle of protected interests and with requirements that are first and foremost directed at legislation, which must consistently develop an appropriate data protection regime and coordinate it with other legal regimes. It is in line with this approach that the ECJ recognises different dimensions of protection, ie, besides rights of defence against encroachments, also duties to protect or, not quite clearly, an indirect horizontal effect in the relationship between private individuals.[156]

Where appropriate, the ECJ points to the provisions of article 8(2) and (3) of the CFR for guidelines. In addition, it bases many requirements on the principle of

[150] ECJ, Judgment (Grand Chamber) Case C-203/15 and Case C-698/15 *Tele2 Sverige* ECLI:EU:C:2016:970, [2016] § 129.

[151] ECJ, Judgment (Grand Chamber) Case C-293/12 and Case C-594/12 *Digital Rights Ireland Ltd* ECLI:EU:C:2014:238, [2014] §§ 29 f, 40, 54.

[152] ECJ, Judgment (Grand Chamber) Case C-511, 512 and Case 520/18, *Quadrature du Net* ECLI:EU:C:2020:791, [2020] § 115; Judgment (Grand Chamber) Case C-623/17, *Privacy International* ECLI:EU:C:2020:790, [2020] § 70.

[153] ECJ, Judgment (Grand Chamber) Case C-293/12 and Case C-594/12, §§ 34 f; Judgment (Grand Chamber) Case C-136/17 GC and Others ECLI:EU:C:2019:773, [2019] § 36; Judgment (Grand Chamber) of 21 March 2024, Case C-61/22, *RL* ECLI:EU:C:2024:251, [2024] §§ 70 ff. See also, emphasising that data and information is addressed while it flows, E Orrù, 'Privacy: Scepticism, Normative Approaches and Legal Protection. A Review of the Theoretical Debate and a Discussion of Recent Developments in the EU' (2022) 52 *DPCE online* 2, 779 (798).

[154] *Cf* ECJ, Judgment (Grand Chamber) Case C-131/12 *Google Spain* ECLI:EU:C:2014:317, [2014] § 80; Judgment (Grand Chamber) Case C-136/17, § 36; Judgment (Grand Chamber) Case C-511, 512 and Case 520/18, §§ 106 ff; Judgment (Grand Chamber) Case C-623/17 §§ 50 ff.

[155] See ECJ, Judgment (Grand Chamber) Case C-362/14, § 72; Judgment (Grand Chamber) Case C-511, 512 and 520/18, §§ 87 ff; Judgment (Grand Chamber) Case C-623/17, §§ 30 ff.

[156] See also O Tambou, *Manuel de droit européen de la protection des données à caractère personnel* (Édition Bruylant, Bruxelles, 2020) 22. For the problem of horizontal effects see J Reinhardt, 'Realizing the Fundamental Right to Data Protection in a Digitized Society' in Albers and Sarlet (n 1) 55 (58 ff).

proportionality, from which it takes a limitation of the restrictions on the protection of personal data 'to what is absolutely necessary'[157] – a catchword from which a range of different precautions to be defined in the event of restrictions is then developed in a not necessarily stringent deduction. The requirements and precautions range from system design provisions and thresholds for the respective processing phase to reservations for judicial review or data security requirements to the right of notification in case of intervention.[158]

The case law of the ECJ thus reveals a multi-dimensional and multifaceted conception of the statements of article 8 CFR, without these already being substantively and doctrinally established. However, a coherent concept cannot be expected either. Not only does the ECJ often remain apodictic in its reasons for its decisions against the background of the different legal cultures in the Member States, but it also cannot take on a role that is completely centralised and hierarchical. There is a need for interplays between the courts in the multi-level system. This is due to the fact that the statements of the fundamental right to the protection of personal data need to be contextualised as soon as we seek to fill it with substance.

ii. Achievements and Challenges of the Right to the Protection of Personal Data as Protected Interest

The right to the protection of personal data places the handling of data and information at the centre of its scope of protection. As a novel right that responds to the challenges of modern society, it is hardly surprising that it has triggered extensive debates among the legal community. Since these debates are to some extent guided by substantial and doctrinal preconceptions that differ from one Member State to another, they vary and diverge quite widely.

On the basis of the previous analysis, it can be stated that the right to the protection of personal data anchored in article 8 CFR is a relatively independent right and not exhausted by a reference to the protection of the respect for private life provided by article 7 CFR. It is also not analogous to the right to informational self-determination. It is not based on the idea of control as an underlying concept and does not provide blanket protection for 'control over one's own data'. Nor is it primarily to be understood as a prohibitive right. On the contrary, it is formulated in such a way that it allows us to move away from the traditional substantive and doctrinal patterns of thought and to break new ground. As a right to protection, article 8(1) CFR can be developed multifariously, as is also shown by paragraphs 2 and 3. It points to the need for shaping and the multifunctional role of legislation, but also to the role of those involved in its implementation. Although it is true that existing secondary data protection legislation has

[157] Settled case law, eg, ECJ, Judgment (Grand Chamber) Case C-746/18 *H. K.* ECLI:EU:C:2021:152, [2021] §§ 38 ff.

[158] ECJ, Judgment (Grand Chamber) Case C-293/12 and Case C-594/12, §§ 53 ff, 68; Judgment (Grand Chamber) Case C-362/14, §§ 91 ff; Judgment (Grand Chamber) Case C-136/17, §§ 49 ff; Judgment (Grand Chamber) Case C-511, 512 and 520/18, §§ 105 ff; Judgment (Grand Chamber) Case C-746/18, §§ 51 ff; Judgment (Grand Chamber) Case C-61/22, §§ 75 ff; Judgment (Full Court) Case C-470/21 *Quadrature du Net* ECLI:EU:C:2024:370, [2024] §§ 67 ff; Judgment (Grand Chamber) Case C-548/21, §§ 84 ff.

played a certain role in the genesis of the right to the protection of personal data,[159] its references to legislation need to be understood dynamically. It is suitable for initialising a complex legal framework that is also designed to be constantly adapted.

However, article 8 CFR remains relatively vague in terms of the protected interests. Its wording merely points to the individual's right to the protection of personal data concerning them and offers some more or less eclectic guidelines in paragraphs 2 and 3. The vagueness of the guidelines, together with the fact that activities are shifting increasingly to the Internet and conflicts are becoming datafied, is leading to an ever-expanding scope of protection in case law. Against this background, the right to the protection of personal data tends to turn into a 'super-fundamental right' within the realm of a 'law of everything'.[160] To avoid this, there have been numerous attempts by jurisprudence and scholarship to clarify what exactly is meant by data protection and what the right to the protection of personal data aims to achieve in contrast to other rights. If, for example, article 7 CFR is interpreted in the case law of the ECJ as protecting private life in a substantive sense, while article 8 CFR focuses on data security or risks of unlawful access and abuse of personal data, or if the right to the protection of personal data is conceptualised as a procedural right, solutions are sought in a functional combination of both rights. But this combination is usually conceived as an additive juxtaposition. Such an additive juxtaposition is not feasible and falls short because it does not succeed in convincingly distinguishing between the scopes of protection of privacy on the one hand and data protection on the other. Furthermore, it is recognised that the right to the protection of personal data also has close interdependencies with other freedoms that contribute substantive aspects. But references to other fundamental rights, such as freedom of expression, remain vague. Again, the relationship between the right to the protection of personal data, the right to privacy, and other substantive freedoms is not convincingly elaborated either in terms of content or doctrine.

IV. Conceptualising Data Protection Interests as a Bundle of Provisions and Rights in a Multilayered Approach

In the following, the considerations on the backgrounds, in particular on the network of basic elements, and the insights from the case law, where partly parallel and time and again more or less convincing solutions can be found, will be brought together. It has become obvious that we need to leave behind approaches that do not do justice to the subject matter. How this can be realised in detail depends on the legal system, on what is enshrined in the Constitution, and on doctrine and methodology. But in the first step, some notes on the essentials of appropriate legal approaches and then an overarching meta-conception shall be introduced.

[159] *Cf* the Explanations on art 8, Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17.

[160] Purtova (n 37).

A. Essentials of Appropriate Legal Approaches

i. Data and Information as Distinct Content of Fundamental Rights Protection

The first finding that can be made in the light of the characteristics of the subject matter, but also in the light of case law, is that protection with regard to the handling of information and data concerning individuals must be conceived as a novel, distinct facet of fundamental rights protection. In the case law on the right to privacy, courts emphasise occasionally that the information and data dimension is a distinct facet. Moreover, such an acknowledgement is the convincing achievement of the FCC's development of the right to informational self-determination and of the enshrinement of a right to the protection of personal data. The fact that there are cross effects between the information and data-related dimension of protection and other facets of fundamental rights protection – protection of decisions, actions, spaces, property – does not undermine this finding.

We cannot assume that it is impossible to develop any rights in this respect. Nor are such rights to be understood as merely accessories to the familiar scopes of protection.[161] On the contrary, developing out data protection interests as a facet of fundamental rights is capable of broadening our narrow notions of protected interests and the philosophical traditions behind them.

ii. Multi-Layered, Multi-Dimensional and Multifaceted Guarantees and Rights

Keeping in mind at what a fundamental level we are dealing with and that a network of fundamental categories is being addressed – data, information, knowledge, processes as data and information flows, and communication – it would be naïve to think that protection of personal data and information could be described in terms of a uniform protected good. The requirement of multi-layered, multi-dimensional, and multifaceted guarantees and rights becomes apparent at many points across the jurisdictions.

The most significant and also most challenging insight is the necessity of a multi-layered conception. At first glance, an extension of the notion of freedom anchored in each fundamental right to the handling of data and information might seem like a good idea. In other words, to embed the protected interests in the context of the entire constitutional law and to search for them at the level of each individual fundamental right. At times, particular guarantees have already been drawn upon. The European

[161] Despite the interrelationships with other facets of fundamental rights protection, it would be misleading to understand protection with regard to the handling of information and data in purely instrumental terms. Of a different opinion G Britz, 'Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts' in W Hoffmann-Riem (ed), *Offene Rechtswissenschaft* (Tübingen, Mohr Siebeck, 2010) 562, 569 ff; R Poscher, 'Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen' in Gander et al (eds), *Resilienz in der offenen Gesellschaft* (Baden-Baden, Nomos, 2012) 167, 178 ff. Slightly broader accentuated Britz (n 116).

Court of Justice mentions the freedom of expression quite regularly. The freedom of assembly has been acknowledged as being relevant in the case of surveillance by intelligence services. The right to mental integrity could be interpreted with regard to the use of certain neurotechniques.

However, if all the possible specific scenarios of the handling of personal data and information are considered, the application of content-specific guarantees turns out to be full of prerequisites. We are not confronted with a single act of intervention but with processes. The contents of the information and the consequences of their use depend on the respective purpose. As data protection is primarily future-orientated, and aims at avoiding harms beforehand in a way that 'we cannot afford to wait to vindicate it only after it has been violated',[162] we must be able to describe to a certain extent which data are collected and how they are altered and linked with one another, which information could be derived from certain data, for which purposes it is used, and which disadvantageous consequences the individual might have to expect. It is therefore necessary to work out the relevant context and to break down the processes of handling information and data to the necessary extent by means of descriptions and prognoses. These prerequisites are not given without further ado.

This problem, which arises from the subject matter we address, can be resolved by distinguishing between two or more levels at which the constitutional requirements are to be developed. Fulfilling the requirements at the basic level can create the conditions that enable us to apply particular guarantees at the second level. From a doctrinal perspective, this can be described as a *cooperation of coordinated fundamental rights within a multilayered conception of guarantees and rights*. Within such a multilayered conception, certain interests of the data subject to be protected must or can be addressed at a basic level and resolved there, in particular through appropriate regulation, while more concrete protection interests that emerge in particular contexts, which, thanks to this regulation, can be described with a sufficient degree of accuracy, may be covered by the guarantees of the specific fundamental rights.

Second, guarantees and rights must be multidimensional. They have to be more diverse than the traditional concept of protection against encroachments because the data subject is to be protected with regard to personal information and data which are generated and processed by others in particular contexts. As has just been explained, appropriate regulation at a basic level is necessary; at this level the state is anything but kept out. Beyond that, protection directed solely at defending against and refraining from processing personal data is insufficient because the data subject may also be interested in personal data being made available so that agencies or private persons have the information at their disposal which they need for a correct decision. And it is just as important that the data subject is informed about the processing of personal data and information and can influence it. Hence, individuals need not only 'negative' or defensive rights but also 'positive' or enabling rights to regulation, to know, to obtain information, to participate, or to exert influence.

[162] Judgment of the Canadian Supreme Court, *R. v Dyment*, [1988] 2 S.C.R. 417, at 23: 'This is inherent in the notion of being *secure* against unreasonable searches and seizures.'

Third, guarantees and rights must be multi-faceted in the sense that their appropriately extended concept of freedom includes a variety of protected interests, each of which has its own characteristics. Protection of fundamental rights in terms of the way in which government agencies or other private parties handle personal information and data is different from the legally protected interests with which we are familiar in the traditional understanding of fundamental rights. The subject matter of protection is not a person's freedom of behaviour or decision, and protection of personal data is also not primarily about protecting a private sphere or what is already existing from informational access by others. People are to be protected with regard to the data and information concerning them as well as to the knowledge developed by others about them and against the repercussions or adverse effects this information and knowledge has or may have. But already, due to the mere fact that data and information are handled and interpreted, government agencies or other private persons are structurally involved in the processing of personal data and information. From a general perspective, ie, leaving aside the special cases, personal data cannot be assigned to the person in question like an object belonging to them. Individualistic patterns of assignment fall short.[163] Reasoning why and to what extent the person to whom data, information, and knowledge refer is to be protected must rather be made from a supraindividual perspective. The protected interests of data subjects have to be conceptualised with regard to the sociality of the individual and to structurally involved counterparts. Hence, they require their own separate patterns of description.

iii. Sophisticated Doctrinal Constructions and Methodologies

The understanding of fundamental rights as multi-layered, multi-dimensional, and multifaceted guarantees and rights is not conceivable without sophisticated doctrinal constructions and methodologies. Classical notions based on a bourgeois-liberal approach and the complementary doctrine that fundamental rights are merely rights of defence against encroachments have dysfunctional prerequisites and limitations.[164] If we fall back on them, we will fail to work out data protection interests and the required regulation appropriately. As has been explained, this is why the right to privacy in case law often falls short of what is needed. But by now, extensions of the functions of the fundamental rights and of the scope of their protection, which go beyond the traditional understanding of fundamental rights, are recognised in many countries. Modern codifications reflect the diversity of dimensions of protection in their catalogues of fundamental rights. Additionally, guarantees of fundamental rights are open to interpretation. By means of sufficiently sound and sophisticated methodologies, they permit an elaboration of diverse dimensions of protection, including positive obligations of the

[163] This does not mean that it is not possible to grant decision-making rights to individuals – but it is one of the means of implementation, not the general overarching approach to understanding data protection rights.

[164] More closely M Albers, 'Realizing the Complexity of Data Protection' in Gutwirth and Leenes and De Hert (eds), *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges* (Dordrecht, Springer, 2014) 213 (216 f).

state to provide a regulatory framework and to protect individuals through legal rules and actions.

iv. Various Functions of Statutory Regulation and Legal Norms

Last but not least, if guarantees and rights have to be understood as multi-layered and multidimensional, legislation is addressed in different roles. It must not only create positive rights of the data subject to know about or to exert influence on the processing of personal data and information but also provide for an appropriate legal framework at a basic level. Legal norms do not only limit freedoms; they can also create freedoms in the first place, make them concrete, and influence their social conditions and prerequisites. The resulting variety of relationships between fundamental rights and statutory regulation can be elaborated in a very nuanced way. The point is not reduced to the idea that a legal basis in the sense of the traditional concept of a defence against encroachments needs to be provided for.[165] On the contrary, developing sophisticated approaches to regulation and its functions is essential. Further considerations can also lead to novel approaches to the understanding of law as such.

B. Cooperation of Fundamental Rights at Different Levels

In summary, data protection rights can be developed from an interplay of fundamental rights within the framework of a multi-layered concept. Such an interplay should not be conceived as an additive juxtaposition. Rather, it must be understood as a *functional cooperation* of fundamental rights at *different* levels. This results in a bundle of multi-layered, multidimensional, and multi-faceted provisions and rights to which all fundamental rights with their substantive particularities can contribute.

i. Basic Level: Provisions and Rights to Appropriate Regulation

At a basic level, data protection responds to risks and harms that have been addressed since the emergence of new technologies in the 1970s and have increased even further with the internet. In a rough summary, the crucial problems centre around a potentially all-encompassing, unlimited, and non-transparent processing of personal data and information by the state or other private parties. These problems are, of course, a question of individual freedom in sociality, but they also point beyond that.[166] Orwell's 'Big Brother', Bentham's 'Panopticon', and Kafka's 'The Trial' might be illustrative as widely known, culturally anchored metaphors that – despite these narratives being rooted in quite different contexts – take up different facets of the dangers just mentioned above. In addition to these state-centred works, more recent novels, such as Dave Eggers' 'The Circle', might be added with a view to social networks.

[165] *Cf* Masing (n 140).
[166] *Cf*, however, the critical remarks made by Masing (n 140).

Daniel Solove has shown that the well-known Big Brother metaphor effectively captures certain data protection problems, but that it is the Kafka metaphor that illustrates those elements of threats to privacy which deal with certain data collection and circulation by others

> without having any say in the process, without knowing who has what information, what purposes or motives those entities have or what will be done with that information in the future.[167]

The very beginning of the work gives a sense of how threatening this can be: 'Someone must have slandered Josef K., for one morning, without him having done anything wrong, he was arrested. Why so, he asks the guards, and receives the terse reply: We are not appointed to tell you that.'

These considerations point to the fact that, at the basic level, there are already multifarious threats that data protection shall countervail. In the first place, they call for the establishment and implementation of a legal framework guaranteeing that the handling of personal information and data is not largely unbound, unlimited, opaque, or beyond any possibility of affected individuals to influence procedures or results. Additionally, as we have already seen, the legal framework at the basic level also has the function of ensuring that contextually definable risks that the data subjects may face are recognisable and describable and of creating the conditions for the applicability of specific fundamental rights. Thus, *substantially*, the regulations directed by certain constitutional guidelines must ensure that data and information flows and contexts of data processing are limited and structured, that data subjects have certain rights of knowledge and of influence, or that there are appropriate institutional provisions. *Functionally*, the regulations must create the conditions that make it possible to apply specific guarantees and ensure, for example, that risks to specific protected interests can be identified and countered in due time.

But is this level and are these requirements covered by fundamental rights and, more closely, by individual rights? That depends, of course, on the legal system in question and on its constitutional provisions, doctrines, and methodologies. It is conceivable that it is up to the legislator to decide whether and to what extent a legal framework is created on the basis of which specific fundamental rights can then be applied and unfolded in a way that reflects the subject matter appropriately. However, in principle, there is no reason to assume that fundamental rights are not suitable for covering this basic level.

In scholarly approaches as well as in the case law of courts, a level that is more foundational than cases that can be contextually delineated is recognised and addressed to a certain extent. It is reflected, for example, in the numerous considerations on the relationship between data protection and a democratic order. Data protection is seen as a factor in, or even a prerequisite for, enabling a democratic order to exist.[168] This presupposes, of course, that it is understood not as individual control over personal

[167] D Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 *Stanford Law Review* 1393, 1426.

[168] See for references to the democratic order BVerfGE 65, 1, 43.

data, but as multilayered, multidimensional, and multifaceted.[169] But even without these references to democracy, some courts have pointed out that privacy, or the right to respect for privacy, which has been extensively elaborated in some jurisdictions, is at the heart of liberty in a modern state and a condition for the enjoyment of other rights or non-discrimination.[170] However, as the right to privacy covers many facets, from preconditions to various protected interests in very specific case constellations, and as the content of the protection is more or less blurred, this cannot be addressed with the necessary accuracy.

Greater clarity and effectiveness can be achieved if these interests of the data subject at this basic level are assigned to a specific fundamental right and its protective content is developed accordingly. With regard to German law, this is possible in view of article 2(1) in conjunction with article 1(1) of the Basic Law if we leave behind the version of the right to informational self-determination that was established by the census ruling and which is now in flux anyway and develop a more complex conceptualisation of the safeguards and individual rights provided by this fundamental right.[171] Even better suited to such an approach is the right of individuals 'to' the 'protection' of personal data concerning them.

The right to the protection of personal data offers the opportunity to work out the content of the protection and the protected interests of the data subjects independently with a fresh approach in terms of content and doctrine, and thus in accordance with the subject matter.[172] Such a right can be interpreted in such a way that it provides regulatory and protective requirements that primarily apply at a basic level prior to constellations that can be contextually delineated and addresses certain protection needs of the data subjects at a first-layer level. Regarding article 8(1) CFR, these considerations are consistent with the fact that article 8(2) and (3) CFR lay down a number of requirements, although these are a rather unsystematic compilation of several factors of different provenance, which do not exhaustively describe the core of the right to the protection of personal data. Article 8 CFR primarily addresses the legislator with a complex set of provisions and, to a certain extent, corresponding individual rights aimed at ensuring that the substantive and functional requirements, as explained above, are met through appropriate regulation.[173]

[169] *Cf* also from an overarching point of view, P de Hert and C Cocito, 'The Added Value of Data Protection within the Framework of Digital Constitutionalism in Europe' in De Gregorio (ed), *The Oxford Handbook of Digital Constitutionalism* (Oxford, Oxford University Press, 2024).

[170] See as examples from our analysis of the case law Supreme Court of Canada, *R. v Dyment*, [1988] 2 S.C.R. 417, at 17; Supreme Court of India, *Puttaswamy-I*, Chandrachud, J, Part R (243, 244); Constitutional Court of South Africa, *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others*; *Minister of Police v Amabhungane Centre for Investigative Journalism NPC and Others* (CCT 278, 279/19) [2021] ZACC 3, at 112 ff.

[171] Albers (n 9) 454 ff. This approach to art 2(1) in conjunction with art 1(1) of the Basic Law is not prior to individual rights but addresses a level precedent to concrete cases covered by specific fundamental rights. It is also at this level that both safeguards and individual rights can be developed.

[172] See also the considerations of P de Hert, ch 12 in this volume, (section VII).

[173] This coincides with many elaborations in the literature – even if they each have their own approaches to a certain extent – that distinguish the right to respect for private life from the right to the protection of personal data and highlight that the latter stipulates that a regulatory framework involving a multi-dimensional set of rules be established, see, eg, P De Hert and S Gutwirth (n 149) 3 ff; M Tzanou, *The Fundamental Right to Data Protection* (Oxford, Hart Publishing, 2017) 7 ff; M von Grafenstein, 'Refining the Concept of the Right

This is not done with any regulation. In particular, and as a non-exhaustive outline, legislation must safeguard that the handling of personal information and data is not unrestricted, unlimited and opaque. It must also provide that risks to specific protected interests of data subjects can be identified and countered in a timely manner. Data subjects must have the opportunity to obtain sufficient knowledge of and influence over the processing of data and information relating to them. Given the inherent limitations of rights-based approaches alone, a number of obligations must be imposed on persons or entities that handle personal information and data. Institutional safeguards and control mechanisms must be added.[174]

Under these circumstances, the pertinent fundamental rights must be interpreted as provisions and rights that are directed at requiring legislation to achieve certain goals and fulfil certain functions. On the one hand, they do not lay down a definite program that simply has to be carried out. Rather, the legislator has a margin of appreciation in the choice of the specific legal measures and instruments, as long as the goals and functions set forth in the Constitution are achieved with the regulation created. On the other hand, precisely because the fundamental rights demand such a result, they would fall short if they were limited to merely vague statements. The problem of the extent to which it is possible to develop provisions and rights that are sufficiently clear to be effective as constitutionally binding from the textually relatively vague fundamental rights is one of the core questions of all interpretations of fundamental rights that go beyond the 'classical' defence against encroachment.

The challenges can be handled if we understand the pertinent fundamental rights in such a way that they consider the regulatory choices of the legislation and are constantly reapplied at more specific stages with more concrete requirements. Thus, as long as there is no legislative framework, fundamental rights requirements initially start with relatively vague provisions and rights. Then, at a second stage, they are conditioned in the sense that they are based on the legislator's regulatory choices of a specific framework and set more specific, concrete provisions for its rules and regulations. In the case law of the German Federal Constitutional Court, there are illustrative examples of such an approach in the areas of the guarantee of property, of the freedom of the press, and, above all, of the freedom of broadcasting.[175] As a result of such a process

to Data Protection in Article 8 ECFR Part I' (2020) 6 *European Data Protection Law Review* 509, 514 ff; M von Grafenstein 'Refining the Concept of the Right to Data Protection in Article 8 ECFR Part II' (2021) 7 *European Data Protection Law Review* 190, 191 ff; and 'Refining the Concept of the Right to Data Protection in Article 8 ECFR Part III' (2021) 7 *European Data Protection Law Review* 373, 374 ff; P Vogiatzoglou and P Valcke 'Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law' in E Kosta, R Leenes and I Kamaras (eds), *Research Handbook on EU Data Protection Law* (Cheltenham and Northampton, Edward Elgar, 2022) 11 ff.

[174] *Cf* Albers (n 164) 229 ff. *Cf* also with partly different considerations, N Marsch, *Das europäische Datenschutzgrundrecht: Grundlagen, Dimensionen, Verflechtungen* (Tübingen, Mohr Siebeck, 2018) 127 ff; L Dalla Corte, 'A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection' in D Hallinan, R Leenes, S Gutwirth and P de Hert (eds), *Data Protection and Privacy: Data Protection and Democracy* (Oxford, Hart Publishing, 2020) 27 (38 ff).

[175] See, eg, the landmark judgment *FRAG* of 1981, BVerfGE 57, 295 (319 ff) [1981] – *Rundfunkentscheidung (Broadcasting freedom judgement)*. Initially, the fundamental right that safeguards broadcasting freedom provides merely general requirements, but no particular model of how to regulate and organise broadcasting. However, if the legislator chooses, for example, a dual model of public and private broadcasting, the guarantee of the freedom of broadcasting sets out more detailed guidelines based on the model chosen by the legislator.

of interpretation, the relation between the pertinent fundamental rights and statutory legislation can be described as being shaped in a way that secondary legislation impacts 'the content of the fundamental right, which is therefore destined to be constantly in flux and evolution'.[176] However, the relation is neither reverse nor a circle. It is important to note that the relative hierarchy between fundamental rights requirements and legal regulations always continues to exist. Altogether, the interplay between fundamental rights and statutory regulations in the field of data protection becomes extremely challenging.

Since the fundamental right to the protection of personal data understood in this way requires, from a functional point of view, that the regulations at the basic level create the conditions that make it possible to apply specific guarantees, it points beyond itself to the spectrum of other fundamental rights.[177] It sets the stage for them to enter the scene.

ii. Second Level: Data Protection Rights from Content-Specific Fundamental Rights

At a second level, content-specific fundamental rights can enter the picture. This applies to all possibly relevant guarantees: rights to mental integrity, to freedom of thought, conscience and religion, to freedom of expression, to freedom of assembly, or to freedom to choose an occupation. In the concept outlined here, if the right to privacy is established alongside a right to the protection of personal data, it can also be given specific content. The factual fundamentals already suggest the recourse to a broad normative basis to concretise fundamental rights requirements. The jurisprudence of the courts, as shown, has in principle recognised the relevance of the specific fundamental rights.[178] However, specific freedoms are often mentioned only in passing. It is not worked out exactly under which conditions they actually apply and how.

Whether, when, and how they are to be applied can be more clearly and precisely defined by considering that the ability to describe all relevant risks to data subjects that may or are likely to arise and the specific interests to be protected requires basic regulations at the first level. If such regulations exist and if we can then describe in more detail the contexts in which the handling of personal information and data takes place, the purposes, the players involved, and the procedures, potential context-specific harms and the particular interests of the data subject to be protected show up. Under these circumstances, specific fundamental rights tailored to particular contexts and risks can be referred to. We can interpret them in a problem-orientated way from a supraindividual perspective, keeping in mind the characteristics of data, information, and

[176] Y Ivanova, 'The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World' in D Hallinan, R Leenes, S Gutwirth and P de Hert (eds), *Data Protection and Privacy: Data Protection and Artificial Intelligence* (Oxford, Hart Publishing, 2021) 145, 151.

[177] In the European multi-level system, the relationship between the EU and its Member States must additionally be addressed, which includes the relationship between the fundamental rights enshrined in the EU Charter and those in the Member States' constitutions. This adds another layer of complexity to the picture, but this will not be discussed in this text.

[178] See nn 90, 91, 106, 155.

knowledge. Provisions and individual rights can be applied exactly where and insofar as a need for protection can be identified. This results in a broad, dynamic, and procedural concept of data protection rights derived from specific fundamental rights.

Legislation regulates the given situation with regard to additional protected interests and can restrict these if necessary. The result is not only a sophisticated arrangement of fundamental rights but also a sophisticated picture of the legal regulations guided by various fundamental rights provisions. This does not have to result in lots of regulations. A specific statutory rule may be shaped by a multitude of different provisions of fundamental rights. This is not unusual, especially not in the multi-level system between the EU and the Member States. In the bigger picture, developing data protection law becomes even more challenging, and this is what I will discuss now in closing.

C. Developing Data Protection Law

Data protection places high demands on law, and regulatory concepts are complex on their own terms. This is all the truer as regulations are shaped not only by fundamental rights and the requirements they impose but also by legal policy. Even if individual rights are developed in a way that reflects the characteristics of data and information and is problem-orientated, they are and should be only a small component of a much larger architecture.[179]

Statutory rules and legal positions of data subjects must be founded on the diverse functions and diverse forms of law. Regulation concepts must include a wide range of constituent elements which utilise the entire spectrum of legal forms and instruments, and in addition, they have to be interwoven. As an innovative and highly dynamic field, data protection law needs to be, in terms of legal theory, 'reflexive law' and, from a doctrinal point of view, a mixture of stability and dynamics. This is reflected, for instance, in the delegation of legislative competences, in the use of legal terms which are vague and in need of being concretised, in normative references to dynamically adapted technical standards, in rules allowing for experimentation, in evaluation procedures, or in other tools to ensure the capacity to learn and develop. In many respects, the appropriate use of insights from other disciplines or interdisciplinary approaches is needed.[180] The emerging variety of regulatory concepts is also compatible with a less legislation-centred understanding of law and regulation. From a political science point of view, it has been analysed how the substance of data protection law is made concrete by the interactions among different actors – the legislative, executive, and judicial branches; data protection agencies; data users; and data subjects. An appropriate normative conception has to be responsive to the interplay of actors generating and concretising law whilst, at the same time, keeping the normative perspective. Last but not least, it is essential to embed data protection rules and rights in overarching contexts and to coordinate them appropriately with other legal regimes.

[179] D Solove, 'The Limitations of Privacy Rights' (2023) 98 *Notre Dame Law Review* 975, 977 ff.
[180] See, eg, A Schimke, *Netz-Gedächtnis und Recht* (Tübingen, Mohr Siebeck, 2025).

How (personal) information and data may be processed has always been regulated, to some extent and from certain perspectives, by various legal regimes such as media law or tort law. The resulting need for coordination between the rules of these regimes and data protection law is increasingly evident, and this is a very challenging task.[181] The same applies to the series of regulations within the EU Data and Digital Strategy. Data protection is, and must be, an integral part of this overall strategy. However, as the GDPR is, to some extent, path-dependent[182] and sticks to traditional patterns of data protection that are not compatible with some of the other regulatory concepts, it cannot remain entirely untouched.[183] As a prerequisite, the fundamental rights and protected interests of data subjects must also be rethought and reconceptualised.

V. Summary and Outlook

This chapter began by drawing attention to the fact that data protection law deals with a highly complex subject matter involving (personal) data, information, knowledge, or processing and, in the broader context, also decisions, actions and their consequences. It aims at protecting individuals, and, in addition, connections to normative principles such as democracy can be identified. The complexity of the issue highlights the challenges that arise not only in the detailed elaboration of data protection law but also in the conceptualisation of the interests to be protected. In this respect, privacy is still a keyword around the world, and the right to privacy is a normative anchor that is, in various formulations, explicitly codified in constitutions or derived from them through interpretation. However, one of the findings of our analysis of case law is that privacy, particularly in law, is burdened with traditional substantive and doctrinal implications that hamper a suitable conceptualisation of data protection. That is why the 'right to the protection of personal data', which has recently been established in some fundamental rights catalogues, offers a fresh opportunity to appropriately conceive and develop such protection in an interplay with other fundamental rights.

Data protection responds to threats to freedom and needs for protection that require their own separate patterns of description. The ensemble of fundamental rights calls for developing a multi-dimensional and manifold bundle of provisions and rights within the framework of a multi-layered conception. This bundle includes, at a basic level, provisions and rights for appropriate regulation, and, at a second level, further

[181] See A Schimke, 'Forgetting as a Social Concept. Contextualizing the Right to Be Forgotten' in Albers and Sarlet (n 1) 179 (190 ff).

[182] Following the path taken by the Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data from 1981 and the EU Data Protection Directive from 1995, see also RD Veit, *Einheit und Vielfalt im europäischen Datenschutzrecht* (Tübingen, Mohr Siebeck, 2023) 103 ff.

[183] In principle, the Commission assumes that the existing data protection regulations, as one of the pillars of its data and digital strategy, can be reconciled relatively seamlessly with the new regulations. *Cf*, eg, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'A European strategy for data' [2020] COM(2020) 66 final. See also art 1(3) Data Governance Act, art 1(3) Data Act. A closer analysis, however, reveals various inconsistencies, incompatibilities and reform requirements.

requirements and rights arising from content-specific fundamental rights. It must be open to continuous revision and constantly adapted to societal change and new threats.

At present, one of the key legal challenges is how data protection law can be convincingly included as part of a comprehensive data and information law, as it is now being addressed in numerous regulations related to the Internet or artificial intelligence. Only a properly tailored approach to data protection interests and data protection law can be reasonably coordinated with other areas of law.