II.
Data Protection and Privacy Rights in the Digital Age

Unfolding the Protected Interests of Data Subjects in Digital Constitutionalism

Marion Albers

Abstract: How to conceptualize the protected interests in data protection law is of crucial interest for digital constitutionalism, as the European Union has adopted a series of new regulations as part of its data and digital strategy. After giving an overview of this strategy to show the extent to which the legal framework is changing, this article provides an in-depth cross-jurisdictional analysis of the right to privacy, the right to informational self-determination, and the right to the protection of personal data. While the details of these rights depend on the specific legal system, their substantive and doctrinal constructions can be distinguished, and a closer analysis reveals particular achievements and weaknesses. Once the factual fundamentals – in particular, data and personal data, information, processing of data and information or knowledge – have been clarified, the need to develop approaches tailored to the characteristics of the handling of personal data and information as a specific dimension of protection becomes obvious. Multi-layered, multi-dimensional and multifaceted guarantees and rights as well as sophisticated doctrinal constructions and interplays between fundamental rights and statutory regulation must be worked out. The last part of this article presents the required doctrinal approach to data protection interests. It is constructed as a functional cooperation of fundamental rights at different levels resulting in a bundle of provisions and rights to which all fundamental rights can contribute with their substantive particularities. Such an approach can be harmonized with the changes in the legal framework brought about by the European data and digital strategy.

A. Introduction

How to conceptualize and describe 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 digitalized, the more this area of law moves from the sidelines to the center of attention. At first glance, the legitimate interests covered by data protection law seem to be clear: right to privacy, right to informational self-determination, or right to the protection of personal data. But these are "umbrella terms"[1] at best. A closer analysis reveals contestable premises, pitfalls, heterogeneous notions and misconceptions. Additionally, the Internet and the social arrangements that it makes possible raise a multitude of more or less novel questions.[2] Both the subject matter and the doctrinal construction of protected interests require clarification and further elaboration.

This article will first provide an overview of the European data and digital strategy to show the extent to which the legal framework is changing, which data protection rights shape as an integral element, but in which they must also be consistently embedded. In the following third section, we will take a look at the familiar, but fuzzy concepts of data protection interests in scholarly debates and in case law. The focus is on the right to privacy, the right to informational self-determination, and the right to the protection of personal data. The in-depth analysis of the achievements and limitations of these different approaches will reveal that the idea of a "right to the protection of personal data" can offer a starting point to address substantial and doctrinal challenges. Further steps can only be reached if we get a clear understanding of the factual fundamentals of data protection, in particular, data and personal data, information, processing of data and information, or knowledge. In the fourth section, I will first explain more closely that data protection deals with a highly complex subject matter. In this light, multi-layered, multi-dimensional and multifaceted guarantees and rights as well as sophisticated doctrinal constructions and interplays between fundamental rights and statutory regulation must be developed. These insights enable us to concretize protected interests of data subjects within a multi-layered conception to which all fundamental guarantees and rights with their substantive particularities can contribute. Such an approach is a prerequisite for coordinating data protection law with other legal regulations in a reasonable way and, for example, embedding it appropriately within the overarching European data and digital strategy.

1 Cf. *Daniel Solove*, Understanding Privacy, 2008, 45.

2 See the manifold articles in *Marion Albers* and *Ingo Wolfgang Sarlet* (eds.), Personality and Data Protection Rights on the Internet, 2022.

B. Reframing Data Protection Interests in Digital Constitutionalism

Since the beginning of this decade, the European Commission has presented numerous proposals for the regulation of data, technologies and infrastructures which are partially captured under the catchword "digital sovereignty"[3]. A crucial part of the Commission's overarching strategies and policies is a comprehensive package for "shaping Europe's digital future".[4] This covers, first of all, the meanwhile implemented regulations on digital markets and digital services.[5] 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 digitization. Within the framework of the data strategy, the data protection regulations – above all the General Data Protection Regulation (GDPR)[6], which is supplemented by the Data Protection Direc-

3 More comprehensive on this catchword *Petra Gehring*, Datensouveränität versus Digitale Souveränität: Wege aus dem konzeptionellen Durcheinander, in: Augsberg/Gehring (eds.), Datensouveränität, 2022, 19 (19 ff.).

4 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" of 23.3.2017, COM(2017) 134 final; "Towards a common European data space" of 25.4.2018, COM(2018) 232 final; "Shaping Europe´s digital future" of 19.2.2020, COM(2020) 67 final; "A European strategy for data" of 19.2.2020, COM(2020) 66 final; "European Commission digital strategy. Next generation digital Commission" of 30.6.2022, COM(2022) 4388 final; White Paper "On Artificial Intelligence – A European approach to excellence and trust" of 19.2.2020, COM(2020) 65 final.

5 Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) of 14.9.2022, O. J. L 265/1; Regulation (EU) 2022/2065 of the European Parliament and of the Council on a single market for digital services (Digital Services Act) of 19.10.2022, O. J. L 277/1.

6 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) of 27.4.2016, O. J. L 119/1.

tive for Police and Criminal Justice[7], by the e-privacy Directive[8] and by further sector-specific legal acts – are classified as a first fundamental pillar intended to provide a "framework for trust in the digital environment"[9]. In the meantime, a whole series of further regulations or regulatory proposals have been added. Complementary to and distinct from the GDPR, but entirely in line with the double finality set out in Art. 1 GDPR, the guiding principle of free data flows is established for non-personal data.[10] Open data concepts, as they are increasingly being enshrined, 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.[11] This aims at enabling not only innovative data-based business models or research, but also joint government-to-business data use, for example in the fields of environmental protection or mobility. The provisions of the regulation on European Data Governance[12] are intended to promote the establishment of sector-specific data spaces, such as the already outlined

7 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, O. J. L 119/89.

8 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 of 12.7.2002, O. J. L 201/37. The debates on an e-privacy regulation are still ongoing.

9 Communication from the Commission "Towards a common European data space" of 25.4.2018, COM(2018) 232 final, p. 1.

10 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 of 14.11.2018, O. J. L 303/59, and the Commission's Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union of 29.5.2019, which in particular deal with the demarcation from the regulations on personal data in the GDPR, COM(2019) 250 final.

11 Directive 2019/1024/EU of the European Parliament and of the Council on open data and the re-use of public sector information of 20.6.2019, O. J. L 172/56; for delimitation in the above context, see Art. 2(1)(h) on its scope.

12 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) of 30.5.2022, O. J. L 152/1.

European Health Data Space[13]. Among other things, these regulations create a framework for "data altruism": 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, i.e., data sharing services that can also operate in the sense of "data trustees", and data altruistic organizations are given a key role with regard to, among other things, ensuring data protection rights. Complementary to the GDPR and the Data Governance Regulation, the Data Act 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. 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.[14] The Cybersecurity Act, which establishes ENISA as an institution and creates certification procedures[15], and the AI-Act, which lays down harmonized rules on artificial intelligence[16], also play an important role in connection with digitization and its regulation.

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.[17] A closer analy-

13 Proposal of the Commission for a Regulation of the European Parliament and of the Council on the European Health Data Space of 3.5.2022, COM(2022) 197 final. Recently, consensus has been reached in the trilogue procedure.

14 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) of 13.12.2023, O. J. L 1/71.

15 Regulation 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) of 17.4.2019, O. J. L 151/15.

16 Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence […] (Artificial Intelligence Act) of 13.6.2024, O. J. L, 12.7.2024.

17 Cf., for example, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of

sis, however, reveals various inconsistencies, incompatibilities and reform requirements. To a certain extent, the GDPR sticks to traditional patterns of data protection and is path-dependent.[18] However, not all of the traditional patterns of thought are convincing and compatible with other regulatory approaches the EU data and digital strategy chooses. Irrespective of this, it becomes clear how importantly and carefully the law governing the handling of personal data and information needs to be embedded in overarching contexts and coordinated with other regulations. In view of the role of data in a digitized society and in view of the new normative models such as open data, the potential of data to create knowledge and value, and common data spaces, the law itself is dependent on dynamic updating. The necessity to develop novel regulatory patterns in data protection requires more clarity about how to conceive of the protected interests.

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

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 U.S. as well as in some other countries such as Canada, India, or South Africa. The understanding of the scope of protection of Art. 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 endeavors to meet the needs of modern society – guarantees everyone the right to the protection of personal data concerning him or her. The following sections analyze these legal foundations with a view to scholarly debates as well as case law and aims at identifying their achievements, weaknesses, and challenges. Last but not least, it will be shown that the

---

the Regions "A European strategy for data" of 19.2.2020, COM(2020) 66 final. See also Art. 1 III Data Governance Act, Art. 1 III Data Act.

18 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 *Raoul-Darius Veit*, Einheit und Vielfalt im europäischen Datenschutzrecht, 2023, 103 ff.

legal concepts are always characterized by substantive as well as doctrinal and methodological considerations.

I. Right to privacy

In many countries, privacy is at the center of debates in various scientific disciplines and public discourse. It seems to be a familiar term, but "privacy" has always been a very heterogeneous concept both in the overarching or academic debates and in case law that recognizes it, in some form, as a constitutionally protected interest.

1. Traditional patterns of thought

A rough overview can highlight some patterns of thought that have been influential in western philosophy, social sciences and jurisprudence. In this context, the traditional understanding of privacy has been shaped by several basic dichotomies[19]: The first of these dichotomies is the contrasting of privacy and the state, which is constitutive for liberal thought. The second dichotomy is the differentiation between privacy and publicness, wherein the concept of "publicness" is conceived in a variety of ways.[20] The third is the differentiation between the individual's private matters and the spheres of decision and influence (also) open to others. This differentiation is linked to one's individuality but is not identical to it. At first sight, these guiding dichotomies seem easy to comprehend, but 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. Due to the complexity of the guiding dichotomies and ideas in the background, this basic notion takes on various nuanced shades of meaning depending on the context and the scientific lens, and privacy touches upon a broad spectrum of topics. Varying across cultures

19 Cf. *Marion Albers*, Privatheitsschutz als Grundrechtsproblem, in: Halft and Krah (eds.), Privatheit. Strategien und Transformationen, 2013, 15 (20).

20 See *Jeff Weintraub*, The Theory and Politics of the Public/Private Distinction, in: Weintraub and Kumar (eds.), Public and Private in Thought and Practice. Perspectives on a Grand Dichotomy, 1997, 1 (1 ff.); *Norberto Bobbio*, The Great Dichotomy: Public/Private, in: Bobbio, Democracy and Dictatorship, 1989, 1 (17).

and historical epochs[21], they 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, or confidential documents and communications.[22] Over time and in a more controversial way, the mechanisms of allocation as one's own and the concept of access have also been understood just as abstractly and broadly. The latter includes invasions of spaces and the body, determination of decisions by third parties, processes of surveillance, or dissemination through the media, and this means that it comprises informational measures.[23] Likewise, "limits to access" are not only spatial in nature. They include physical boundaries, but also boundaries based on social expectations of expectations. Meanwhile, and in response to societal change, privacy has become a more and more differentiated concept which is fleshed out not only by substantial but also by functional approaches.[24] Against this background, it is understood as an "umbrella term".[25]

Classical concepts of privacy and traditional notions of fundamental rights are closely intertwined at several levels. This is true even for basic levels. Liberal thought on fundamental rights presupposes a differentiation between bourgeois or private society and the state. In addition, the structure of fundamental rights provisions reflects the differentiation between private matters of the individual, which *prima facie* enjoy protection based on fundamental rights, and the interests of other citizens or the general public, which can only take effect through passing a law. The protected persons, in turn, can subject state action to judicial review employing the standard of fundamental rights. Thus, we may say that the form of law itself guarantees privacy in the form of subjective rights. Besides these basic levels, there are

21 There is "no *single* history about what is private", *Beate Rössler*, Der Wert des Privaten, 2001, 15.

22 Cf. with a broad historical overview the contributions in *Philippe Ariès* and *Georges Duby*, Histoire de la vie privée, Vol. 5, 1985–1987.

23 See the description of *privacy* by *Sissela Bok*, Secrets – On the Ethics of Concealment and Revelation, 1983, 10 f.: "the condition of being protected from unwanted access by others – either physical access, personal information, or attention".

24 Cf., for example, *Ruth Gavison*, Privacy and the Limits of Law, 89 Yale Law Journal 421, 440 ff. (1980); *Helen Nissenbaum*, Privacy in Context. Technology, Policy, and the Integrity of Social Life, 2010, 74 ff.

25 *Solove* (n 1). Cf. also more closely *Bert-Jaap Koops, Bryce Newell, Tjerk Timan, Ivan Skorvanek, Tom Chokrevski* and *Maša Galič*, A Typology of Privacy, 38 University of Pennsylvania Journal of International Law, 483, 491 ff. (2017); *Sohail Aftab*, Comparative Perspectives on the Right to Privacy, 2024, 39 ff.

numerous thematic overlaps. Fundamental rights cover different protected goods which have often been classified under an overarching concept of privacy. This includes the inviolability of home or correspondence, freedom of religion or freedom of thought, or property.

As there are all these different strands covering a rich tradition, the development of a general right or more specific "rights to privacy" is quite suitable for consensus. The heterogeneous framings and the shifting meanings of privacy make it easier to refer to seemingly established viewpoints, just as they are often the reason for talking past one another. On closer analysis, it depends, of course, on the specific legal system and codification how to interpret constitutional provisions in terms of a "right to privacy". Sometimes such a right is derived on the basis of methodologically substantiated arguments; sometimes there are explicit textual anchors. Our overview of case law begins with the U.S., a cradle of a "right to privacy".

2. 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 conceptualized in detail, is part of a broad debate in the U.S. 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"[26], 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 U.S. Constitution, there are various approaches in the jurisdiction to anchor its more or less specified protection with regard to guarantees of primarily the First[27], Fourth[28], Fifth[29], and Fourteenth[30] Amendments in a

26 *Samuel D. Warren/Louis D. Brandeis*, The Right to Privacy, 4/5 Harvard Law Review 193 (1890).

27 "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."

28 "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."

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

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

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.[31]

In several judgments of the U.S. 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 [...]"[32]. 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".[33] This hereafter acknowledged "right of personal privacy includes the interest in independence in making certain kinds of important decisions".[34] Such decisional privacy is not assigned solely to liberty[35] 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"[36]. 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

31 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).

32 *Griswold v Connecticut* 381 US 479, 485 (1965).

33 *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 U. S. Supreme Court´s judgment of June 24, 2022, *Dobbs v. Jackson Women Health Organization*, with as yet not fully foreseeable ramifications.

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

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

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

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 [...]"[37] characterized 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"[38] would be required for the approval of a relevant encroachment. In response to changes in the way society communicates, the U.S. Supreme Court reached the landmark decision *Katz v United States*[39]: 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"[40], along with

37 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 ...".

38 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.

39 *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.

40 *Katz v. United States*, 389 U.S. 347, 351 (1967).

the "reasonable expectation of privacy" test[41] 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 fulfills 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.[42] 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.[43] 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

41 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.

42 Cf. *Gavison* (n 24), 445.

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

cases.[44] This becomes particularly evident in *Carpenter v United States*.[45] 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.[46] The four dissents presented a variety of arguments which spanned from fundamental criticism of the *Katz* test[47] to the insistence on "accepted property principles as the baseline for reasonable expectations of privacy"[48] 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[49].

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[50], even though the grounds of this judgment were fluctuating when locating these interests within

44 For example, whether "reasonable expectations of privacy" can be recognized, 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.

45 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).

46 *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.

47 See the dissent of Justice *Thomas* in *Carpenter v United States,* 585 U. S. _____ (2018).

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

49 Dissent of Justice *Gorsuch*, *Carpenter v United States,* 585 U. S. _____ (2018), p. 13.

50 *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.

the Constitution.[51] Besides the interest in independence in making certain kinds of important decisions, the individual interest in avoiding disclosure of personal matters was identified.[52] 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.[53] 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.[54] This line of reasoning was sharply criticized by the concurring opinions.[55] 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 U.S. Supreme Court, "privacy" offers only limited, mostly accessory informational protection. Although some of the decisions address digital devices or advanced surveillance methods[56], there is little success in developing sophisticated concepts of the protection that is constitutionally guaranteed. As the grounds of the recent judgment *Dobbs v. Jackson Women Health Organization* may illustrate[57], the reasons for this have to do with the limits of the legal anchors and the methodological strategies. Catchphrases such as "dignity versus liberty"[58] cannot capture the entire background and would be an exaggeration.

---

51 *Carmel Shachar* and *Carleen Zubrzycki*, Informational Privacy After *Dobbs*, 75 Alabama Law Review 1, 12 ff. (2023).

52 *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.

53 *NASA v. Nelson*, 562 U.S. 134 (2011).

54 A lot of questions remain unclear in the grounds, cf. *Christina P. Moniodis*, Moving from *Nixon* to *NASA*: Privacy´s second strand – A right to informational privacy, 15 Yale J. L. & Tech. 139, 157 ff. (2012).

55 Concurring opinion of Justice *Scalia*, joined by Justice *Thomas*.

56 See, for example, 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).

57 *Dobbs v. Jackson Women Health Organization*, judgment of June 24, 2022. The majority judgment emphasizes 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, for example, *Sam Kamin*, Katz and Dobbs: Imagining the Fourth Amendment Without a Right to Privacy. 101 Texas Law Review Online 80 (2022).

58 Cf. *James Q. Whitman*, The Two Western Cultures of Privacy: Dignity versus Liberty, 113 Yale L.J. 1151 (2004).

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[59] – are quite similar to those in the U. S. The understanding of the Charter as a "purposive document"[60] whose spirit "must not be constrained by narrow legalistic classifications based on notions of property"[61] leads to an abstract and broad understanding of Section 8 in the sense of a "right to privacy"[62] that is shaped by the "underlying values of dignity, integrity and autonomy"[63]. The pattern of "reasonable expectations of privacy" has been essential for this understanding[64] and normatively assessed with a view to the "totality of circumstances"[65]. The approach is sufficiently flexible to allow a distinction to be made between "types of privacy interests – territorial, personal, and informational".[66] 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 case of intimate details on the individual's lifestyle and personal choices.[67] Recent judgments go further, differentiating privacy as secrecy, as control and as anonymity[68], and pointing to "informational self-determination".[69] Some cases give rise to the development of more

59 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."

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

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

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

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

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

65 *R. v. Tessling*, 2004 SCC 67, at 31 ff.

66 *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.

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

68 *R. v. Spencer*, 2014 SCC 43, at 38.

69 *R. v. Jones*, 2017 SCC 60, at 39, quoting *R. v. Dyment* and the report of the Task Force, Privacy and Computers, 1972, p. 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 *Alan F. Westin*, Privacy and Freedom, 1970, p. 7: "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent

specific considerations which reflect the characteristics of information. 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."[70] 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"[71], 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 centers on the problem of determining the information content of IP addresses.[72] 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 U. S. 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.[73] Both judgments dealt with the constitutionality of the Aadhaar project, a centralized nation-wide identifi-

information about them is communicated to others". Cf. for the jurisdiction of the German FCC section C. II. of this article.

70 *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."

71 *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.

72 *R. v. Bykovets*, 2024 SCC 6.

73 *Justice K.S. Puttaswamy (Retd) vs 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 K.S.*

cation system based on biometric technology. The Court highlights that privacy "constitutes the foundation of all liberty" and "lies across the spectrum of protected freedoms".[74] In its conclusions, it anchors the right to privacy on a broad foundation: "Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 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."[75] Different strands are covered, among others, informational privacy.[76] It is in line with the multi-layered and broad approach that the right to privacy is not only conceptualized as a right of defense against encroachments. It also includes duties of the state and mandates it to "put in place a positive regime".[77] 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".[78]

What shape does a right to privacy take when it is explicitly enshrined in constitutional codifications? Textually and systematically, it 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.[79] 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 rela-

---

Puttaswamy (Retd) vs Union Of India, Judgment on 26 September 2018, AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018).

74 *Puttaswamy-I*, Part R (p. 243, 244).

75 *Puttaswamy-I*, Part T (p. 266). Already in earlier case law, the right to life enshrined in Article 21 of the Constitution has been interpreted as a basic right to a decent existence. Cf. also regarding the jurisdiction of the Supreme Court of Pakistan *Aftab* (n 25), 99 ff.

76 See *Puttaswamy-I*, Part S (p. 246 ff.).

77 *Puttaswamy-II*, Part G (p. 232); cf. also *Puttaswamy-I*, Part S (p. 254).

78 *Puttaswamy-I*, Part S (p. 246 ff., 252).

79 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.

tively 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.[80] 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 thinking patterns are also at work when it comes to issues of protection of personal data.[81]

Art. 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.[82] 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 decisions increasingly interact[83], it has moved away from the traditional understanding of the ECHR in terms of international minimum standards. According to its case law, Art. 8 ECHR protects a broad spectrum of interests. 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

80 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.

81 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.

82 "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."

83 *Marion Albers*, Höchstrichterliche Rechtsfindung und Auslegung gerichtlicher Entscheidungen, in: Grundsatzfragen der Rechtsetzung und Rechtsfindung, VVDStRL Bd. 71, 2012, 257 (272 ff., 287 ff.).

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 recognized, 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 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.[84] 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 or the IP address, but also photos and video recordings or DNA samples as data carriers.[85] Data processing steps are differentiated and, if necessary, independently assessed as an intrusion.[86] 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 data is sensitive or whether the data subject has suffered specific disadvantages.[87] However, potentially detrimental consequences do play

84 Cf. ECtHR, No. 27798/95, 16.2.2000 – *Amann*, Rn. 44 ff., 64 ff.

85 Cf. ECtHR, No. 20383/04, 12.12.2013 – *Khmel*, Rn. 41 ff., 49; No. 931/13, 27.6.2017 – *Satakunnan*, Rn. 133 ff.; No. 66490/09, 27.2.2018, - *Mockutė*, Rn. 93 f.; No. 62357/14, 24.4.2018 – *Benedik*, Rn. 100 ff., 107 ff.; No. 50001/12, 30.1.2020 – *Breyer*, Rn. 76 ff.; No. 75229/10, 14.4.2020 – *Dragan Petrović*, Rn. 69, 79.

86 ECtHR, No. 20383/04, 12.12.2013 – *Khmel*, Rn. 40 ff.; No. 42788/06, 26.1.2017 – *Surikov*, Rn. 75, 84 ff.; No. 931/13, 27.6.2017 – *Satakunnan*, Rn. 134 ff.

87 ECtHR, No. 28 341/95, 4.5.2000 – *Rotaru*, Rn. 42 ff.; No. 44 647/98, 28.1.2003 – *Peck*, Rn. 57 ff.; No. 62 332/00, 6.6.2006 – *Segerstedt-Wiberg*, Rn. 69 ff.; No. 30 562/04, 4.12.2008 – *S. and Marper*, Rn. 58 ff.; No. 11519/20, 4.7.2023 – *Glukhin*, Rn. 67 ff. See also for a legal obligation of Telegram to decrypt Internet communications if they are encrypted No. 33696/19, 13.2.2024 – *Podchasov*, Rn. 58.

a role in the overall assessment of protection.[88] When such effects are taken into account, other freedoms may become relevant as well, for example the freedom of expression.[89]

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 recognizing 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.[90] And the state does not adequately fulfill 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.[91] Art. 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.[92]

3. Achievements and weaknesses 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 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. How this is done in detail depends 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 protected interest when it comes to constitutionalizing the protection of personal data can be identified which emerge as issues across jurisdictions.

88 ECtHR, No. 931/13, 27.6.2017 – *Satakunnan*, Rn. 137; No. 50001/12, 30.1.2020 – *Breyer*, Rn. 74 ff.; No. 11519/20, 4.7.2023 – *Glukhin*, Rn. 65 ff.; No. 33696/19, 13.2.2024 – *Podchasov*, Rn. 51 ff.

89 See ECtHR, Nos. 58170/13, 62322/14 and 24960/15, 25.5.2021 – *Big Brother Watch*, Rn. 442 ff.

90 ECtHR, No. 47143/06, 4.12.2015 – *Zakharov*, Rn. 228 ff., Nos. 58170/13, 62322/14 and 24960/15, 25.5.2021 – *Big Brother Watch*, Rn. 322 ff.; No. 33696/19, 13.2.2024 – *Podchasov*, Rn. 63 ff.

91 Cf. ECtHR, No. 61496/08, 5.9.2017 – *Bărbulescu*, Rn. 115, 120 ff.

92 ECtHR, No. 10 454/83, 7.7.1989 – *Gaskin*, Rn. 37; No. 62 332/00, 6.6.2006 – *Segerstedt-Wiberg*, Rn. 99 ff.

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. 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 emphasizing that privacy is a crucial value for a liberal society and, in the sense of a pre-condition, essential for the exercise of other freedoms.[93] 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[94] – 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 emphasizes that an impairment does not depend on whether concrete disadvantages have arisen. The data subject as fundamental right's 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 the protection of personal data and freedoms of decisions or behavior that might be protected by specific fundamental

93 See, for example, the Supreme Court of Canada, *R. v. Dyment*, [1988] 2 S.C.R. 417, at 17 (quoting *Alan F. Westin*, Privacy and Freedom, 1970, p. 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 (p. 243, 244).

94 Cf. the dissent of Justice *Gorsuch*, *Carpenter v United States,* 585 U. S. _____ (2018), p. 13, with the proposal to revisit the "kind of legal interest" that "is sufficient to make something *yours*".

rights show up.[95] In this sense, the right to privacy always points beyond itself.

Following traditional patterns for the development and justification of the protection of personal data 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-oriented 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 "defense 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 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 understand their role to be an active one and 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 legislator. While the lines of reasoning are problem-oriented, they may be criticized for not being sufficiently grounded in the provisions, especially since the concept of privacy itself is under constant criticism.[96] 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 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

95 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, 25.5.2021 – *Big Brother Watch*, Rn. 442 ff.

96 See, for example, *Jeffrey Belley*, Pure Privacy, 116 Nw. U. L Rev. 463 (2021).

Federal Constitutional Court, this right has been developed not least in response to the weaknesses of the formerly recognized 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.

II. 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.

1. Approaches and developments in case law

The Federal Constitutional Court derived the "right to informational self-determination" from Art. 2 (1) in conjunction with Art. 1 (1) of the Basic Law[97] in its decision concerning the census (*Volkszählungsurteil*) taken in 1983.[98] 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 Art. 2 (1) in conjunction with Art. 1 (1) of the Basic Law have long been interpreted in the case law of the Federal Constitutional Court primarily as a "right to respect for privacy". Scholarly contributions 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 "privacy" employing the spatial imagery of areas of retreat walled off from the outside world or situations for interaction and communication which 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:

97 Article 2 GG: "Everybody shall have the right to the free development of his or her personality [...]"; Article 1 GG: "Human dignity shall be inviolable. To respect and to protect it shall be the duty of all state authority."

98 Decisions of the FCC, Vol. 65, 1.

the protection of medical files stored at the doctor's workplace from access by security authorities,[99] the use of secret tape recordings in a civil court proceeding,[100] the publishing of a fictitious interview about private matters in the press,[101] or a television movie about a murder in which the criminal, who has since been released, can be identified (the famous *Lebach*-case)[102].

But then the *Eppler*-case resulted in a turning point.[103] 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 Art. 2 (1) in conjunction with Art. 1 (1) of the Basic Law.[104] 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.[105] 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 himself or herself the disclosure and use of his or her personal data.[106] Individuals have the right to decide themselves whether and how their personal data is to be revealed and used, in other words: a right to self-determination about processing of data relating to them. How did the Federal Constitutional Court arrive at this subject matter to be protected? An analysis of the broader background, previous case law and scientific

99 Decisions of the FCC, Vol. 32, 373; Vol. 44, 353.
100 Decisions of the FCC, Vol. 44, 238.
101 Decisions of the FCC, Vol. 34, 269 – *Soraya*.
102 Decisions of the FCC, Vol. 35, 202 – *Lebach*.
103 Decisions of the FCC, Vol. 54, 148 – *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.
104 Decisions of the FCC, Vol. 54, 148, 153 ff.
105 Decisions of the FCC, Vol. 54, 148, 155.
106 Decisions of the FCC, Vol. 65, 1, 43. Analyzing the decision and its background *Marion Albers*, Informationelle Selbstbestimmung, 2005, 151 ff.

debate can explain this very well. 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 U.S.-American privacy debate. The first point of criticism emphasized the relativity of the sphere of personal privacy: it could be described only in terms "relative" to those receiving information.[107] 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.[108] 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.[109] In other words, what is decisive is not the context 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 centers on individual decision capacities as well as on the context of use of personal data.[110] 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 behaviors may be stored as information and used to their disadvantage, they will try not to attract attention by such behavior and are no longer free to act at will.[111] 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"

107 See *Bernhard Schlink*, Das Recht der informationellen Selbstbestimmung, Der Staat 25 (1986), 233, 242; *Daniel Solove*, The digital person, 2004, 212 f.

108 *Alan F. Westin*, Privacy and Freedom, 6th ed. 1970, p. 42.

109 See *Spiros Simitis*, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, 673, 680.

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

111 Decisions of the FCC, Vol. 65, 1, 43.

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[112], but that right is accessory in the context of the concept.

In the course of its case law, the FCC has developed a multitude of requirements statutory law has to comply with. These include the principles of purpose specification and purpose limitation, thresholds for the permissibility of data processing steps, or data security standards. Particular requirements can usually be traced back to the challenges raised by the case. The doctrinal reference point is often 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.[113] 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."[114] 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.[115] In relation to the state, the problem has arisen in cases such as electronic profiling and searches or automatic license plate recognition that personal data is collected but quickly 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 informa-

112 Decisions of the FCC, Vol. 65, 1, 46.

113 For these changes see Decisions of the FCC, Vol. 97, 125, 146 ff.; 97, 391, 403 ff.; 101, 361, 382; 120, 180, 199.

114 FCC, Judgment of 15 December 1999, 1 BvR 653/96 – *Caroline I*, para. 70, https://www.bverfg.de/e/rs19991215_1bvr065396en.html.

115 Cf. *Marion Albers,* Grundrechtsschutz der Privatheit, DVBl 2010, 1061, 1065 f.

tional self-determination in a more or less well thought-out manner.[116] In the *Right to be Forgotten I*-Judgment of 2019, the Court has undertaken significant changes: Between private parties[117], 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"[118]. Further elaboration of the right to informational self-determination continues to progress.

2. Achievements and limitations 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 characterized by an approach that places the handling of personal data and information as such at the center 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.

116 See Decisions of the FCC, Vol. 115, 320, 342 ff.; 120, 378, 398; 150, 244, Rn. 41 ff.

117 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 *Laura Schertel Mendes*, Schutz vor Informationsrisiken und Gewährleistung einer gehaltvollen Zustimmung, 2015, 44 ff. Cf. also for the doctrine of the "Drittwirkung" *Marion 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, 2018, 177 ff.

118 FCC, Order of 6. November 2019, 1 BvR 16/13 – *Recht auf Vergessen I*, Headnote 3 and Rn. 83 ff., https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en.html.

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 likewise a property right.[119] Similar to some U. S.-American conceptions of privacy, informational self-determination is primarily thought of as a right of control over personal data.[120] 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 creating constantly changing data and information is lost. 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 the clarity and

119 Sometimes it is emphasized that the FCC 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", Decisions of the FCC, Vol. 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.

120 The ideas of *Alan F. Westin*, Privacy and Freedom, 6th ed. 1970, 42, which the FCC adopted, have also been cited in some rulings of the Canadian Supreme Court. See also *Charles Fried*, Privacy, 77 Yale Law Journal 475, 482, 483 (1968): "Privacy […] is the *control* we have over information about ourselves […] is control over knowledge about oneself."

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 multilayered as well as manifold and requires a multitude of regulatory tools.

The right to informational self-determination is quite popular in other countries' jurisdictions, as well as in the international scientific community. But we must be aware that the FCC has meanwhile revised its approach, only to a limited extent in the state-citizen relationship, but 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 meanwhile also doctrinally justified[121], opens up opportunities for the necessary further development of fundamental rights.

III. Right to the protection of personal data

Aiming at being a modern charter covering contemporary challenges, Art. 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 him or her.[122] Art. 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.[123] The explicit

121 Cf. *Albers* (n 83), 287 ff.

122 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, Artt. 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*, Rn. 120.

123 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

enshrinement of a right to the protection of personal data has been the model for the new similar anchor in Art. 5 LXXIX of the Constitution of the Federative Republic of Brazil.[124] Art. 8(1) CFR stands alongside the protection of Art. 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?

1. Approaches and developments in case law

In its initial decisions, the ECJ stated that Art. 8 CFR was "closely linked" to Art. 7 CFR[125], and did not differentiate in more detail between the two fundamental rights.[126] Specific difficulties in distinguishing between the scope of protection of Art. 7 CFR on the one hand and Art. 8 CFR on the other arise for doctrinal reasons: Art. 52(3) CFR grants the rights of the Charter the same meaning and scope as the corresponding Convention rights and Art. 7(1) CFR corresponds to Art. 8(1) ECHR which is the foundation of data protection in the case law of the ECtHR. It was the landmark *Tele2 Sverige*-judgment that partially addressed this problem and at least emphasized the distinct nature of Art. 8 CFR. As long as the European Union has not acceded to the ECHR, the ECJ explains, that "Art. 52(3) CFR does not preclude Union law from providing protection that is more extensive than the ECHR" and that Art. 8 CFR "concerns a fundamental

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."

124 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 in May 7, 2020, that paved the way for Congress to pass the constitutional amendment *Ingo Sarlet*, The Protection of Personality in the Digital Environment, in: Albers and Sarlet (n 2), 133 (137 ff.).

125 ECJ, Judgment (Grand Chamber) of 9.11.2010, C-92, 93/09, *Schecke*, Rn. 47.

126 See ECJ, Judgment (Grand Chamber) of 9.11.2010, C-92, 93/09, *Schecke*, Rn. 45 ff.; Judgment (Grand Chamber) of 24.11.2011, Rs. C-468, 469/10, *ASNEF/FECEMD*, Rn. 41 ff. For more in-depth analyses of earlier case law *Paul De Hert* and *Serge Gutwirth*, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in: Gutwirth et. al. (eds.), Reinventing Data Protection?, 2009, 29 ff.

right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR".[127]

However, the Court's interpretation of the scope of protection under Art. 8 CFR does not provide much substance. The *Digital Rights Ireland*-judgment indicates that Art. 7 CFR protects private life in a substantive sense, while Art. 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.[128] The constituent elements of Art 8(1) CFR are "personal data" and their processing, irrespective of whether the information that can be obtained from the data is of sensitive nature or whether any detrimental effects have been suffered.[129] Data processing phases are differentiated and assessed separately – not in isolation, however, but as relatively independent elements of a processing sequence.[130] 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 behavior, against the undermining of professional secrecy or informant protection, or against data misuse.[131] 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.[132] This is quite convincing if we associate Art. 8 CFR with a bundle of protected interests

127 ECJ, Judgment (Grand Chamber) of 21.12.2016, C-203/15 u. C-698/15, *Tele2 Sverige*, Rn. 129.

128 ECJ, Judgment (Grand Chamber) of 8 April 2014, C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, Rn. 29 f., 40, 54.

129 ECJ, Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18, *Quadrature du Net*, Rn. 115; Judgment (Grand Chamber) of 6 October 2020, C-623/17, *Privacy International*, Rn. 70.

130 ECJ, Judgment (Grand Chamber) of 8 April 2014, C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, Rn. 34 f.; Judgment (Grand Chamber) of 24 September 2019, *GC and Others*, C-136/17, Rn. 36; Judgment (Grand Chamber) of 21 March 2024, *RL*, C-61/22, Rn. 70 ff.

131 Cf. ECJ, Judgment (Grand Chamber) of 13 May 2014, *Google Spain,* C-131/12, Rn. 80; Judgment (Grand Chamber) of 24 September 2019, *GC and Others*, C-136/17, Rn. 36; Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18, *Quadrature du Net*, Rn. 106 ff.; Judgment (Grand Chamber) of 6 October 2020, C-623/17, *Privacy International*, Rn. 50 ff.

132 See ECJ, Judgment (Grand Chamber) of 6 October 2015, *Schrems I*, C-362/14, Rn. 72; Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18,

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 recognizes different dimensions of protection, i.e. besides rights of defense against encroachments also duties to protect or, not quite clearly, an indirect horizontal effect in the relationship between private individuals.[133]

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 proportionality, from which it takes a limitation of the restrictions on the protection of personal data "to what is absolutely necessary"[134] – 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.[135]

The case law of the ECJ thus reveals a multi-dimensional and multi-faceted conception of the statements of Art. 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 centralized 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 contextualized as soon as we seek to fill it with substance.

Quadrature du Net, Rn. 87 ff.; Judgment (Grand Chamber) of 6 October 2020, C-623/17, *Privacy International*, Rn. 30 ff.

133 For the problem of horizontal effects see *Jörn Reinhardt*, Realizing the Fundamental Right to Data Protection in a Digitized Society, in: Albers and Sarlet (n 2), 55 (58 ff.).

134 Settled case law, for example, ECJ, Judgment (Grand Chamber) of 2 March 2021, C-746/18, *H. K.*, Rn. 38 ff.

135 ECJ, Judgment (Grand Chamber) of 8 April 2014, C-293/12 and C-594/12, *Digital Rights Ireland Ltd*, Rn. 53 ff., 68; Judgment (Grand Chamber) of 6 October 2015, C-362/14, *Schrems I*, Rn. 91 ff.; Judgment (Grand Chamber) of 24 September 2019, *GC and Others*, C-136/17, Rn. 49 ff.; Judgment (Grand Chamber) of 6 October 2020, C-511, 512 u. 520/18, *Quadrature du Net*, Rn. 105 ff.; Judgment (Grand Chamber) of 2 March 2021, C-746/18, *H. K.*, Rn. 51 ff.; Judgment (Grand Chamber) of 21 March 2024, *RL*, C-61/22, Rn. 75 ff.

2. 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 center 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 Art. 8 CFR is a relatively independent right and not exhausted by a reference to the protection of the respect for private life provided by Art. 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, Art. 8(1) CFR can be developed multifariously, as is also shown by paras. 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 played a certain role in the genesis of the right to the protection of personal data[136], its references to legislation need to be understood dynamically. It is suitable for initializing a complex legal framework that is also designed to be constantly adapted.

However, Art. 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 him or her and offers some more or less eclectic guidelines in para. 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 has a tendency to turn into a "super-fundamental

136 Cf. the Explanations on Art. 8, Explanations relating to the Charter of Fundamental Rights, 14 December 2007, O. J. C 303/17.

right" within the realm of a "law of everything"[137]. 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, Art. 7 CFR is interpreted in the case law of the ECJ as protecting private life in a substantive sense, while Art. 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 conceptualized 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 protection of personal data on the other. Furthermore, it is recognized that the right to the protection of personal data also has close interdependencies with other freedoms that contribute substantive aspects, so that it is no longer clear how privacy and other substantive freedoms relate to each other.

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 in terms of content and doctrine, and thus in accordance with the subject matter. For this to succeed, it is first necessary to reach an understanding of both the factual bases and the essential consequences that must be considered in legal approaches. The right to the protection of personal data can then be convincingly developed and embedded in an appropriate overarching concept.

D. Shaping Data Protection Interests as a Bundle of Provisions and Rights

I. Factual fundamentals

1. 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. Due to technical developments, and also due to the extension of

137 *Nadezhda Purtova*, The law of everything. Broad concept of personal data and future of EU data protection law, 10 Law, Innovation, and Technology 40 (2018).

data protection law itself, uncertainties are reflected in numerous problems: How does the law deal with the manifold descriptions in the various scientific disciplines? Are the terms "data" and "information" synonymous or should they be strictly differentiated? Or is this question, from a practical point of view, of no importance? Which entity can be delimited as a data unity when we step out of the familiar terrain and are not dealing with easily describable situations, but with, for example, big data or AI-contexts? Is data a suitable reference point for the desired legal protection at all?

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". On a very abstract level, data can be understood against the background of the possibilities of differentiation.[138] Such an approach can capture different levels of abstraction and reference points as well as a wide range of applications for the concept of data: the distinguishability of real-world phenomena, physical parameters measured by standards, numbers, letters, texts, communication elements, or binary digital units. The heterogeneity of this non-exhaustive list reveals that the concept of data is a construction that varies according to historical epoch, perspective, and framing. While in a certain phase "data" was often linked to the evolution of science, experimentation and measurement, today they are a multifaceted element of the "onlife"-world. Additionally, the storage forms and data formats in which data is embodied are shaped by the technologies, media and infrastructures.

As the concept of data is a construction, the various scientific disciplines each take their own approach. Concepts of "data", as well as of "information", are described in multifarious and discipline-dependent ways.[139] The law does not simply borrow descriptions like those approaches in 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

138 *Luciano Floridi*, Information. A Very Short Introduction, 2010, 23: "[…] 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."

139 *Floridi* (n 138), 19 ff.

different areas of law such as data protection law, copyright law, or patent 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".[140] How data is to be understood in data protection law must be approached by simultaneously considering "personal data".

2. What is personal data?

Personal data is, as Art. 8(1) CFR describes, data concerning the individual. 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 addresses these questions by defining that the data must relate to either an identified or an identifiable person.[141] 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.[142] If a reference to the person to be protected can only be

140 See, e. g., Art. 2(1) GDPR.

141 Art. 4 no. 1 GDPR.

142 See also the breadth of the term "personal data" ECJ, Judgment of 19 October 2016, C-582/14, *Breyer*, Rn. 32 ff.; Judgment of 20 December 2017, C-434/16, *Nowak*, Rn. 27 ff.; Judgment of 22 June 2023, C 579/21, *J. M.*, Rn. 41 ff.; Judgment of 9 November 2023, C-319/22, *Gesamtverband Autoteile-Handel e. V.*, Rn. 44 ff. Cf. also the overly broad approach of the Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136.

established via 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.[143] This already results 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 exist 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-oriented 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 taken into account 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 end up being a "law of everything"[144].

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 judgments and assumptions of probability come into play. To a considerable extent, prognoses and typifications may enter the

143 See the above mentioned 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.

144 See n 137.

picture. The personal-relatedness of data is regularly not to be 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 conceptualized 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 way around: the reasons for protection make it possible to determine the personal-relatedness of data. 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.

3. 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: 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 and consequences of decisions. Data protection aims at regulating data processing, 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.[145] This is true even though legal definitions and some scholarly contributions might not reflect this in the required manner. Our analysis has shown that several court decisions illustrate this necessity very well. In the first step, data and information must be strictly differentiated, and in the second step, their relationship to each other must be worked out on the level of abstrac-

145 More closely *Albers* (n 106), 87 ff.

tion or concretion that is necessary. Otherwise, neither the characteristics of data protection law nor the challenges it faces can be worked out.

Data protection law addresses data, on the one hand, as an objectified entity. Data might be described as characters or symbols 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. Data, forms of storage, and processing operations are shaped by the various media, technologies, and infrastructures. Against the backdrop of complex digitized processing, "virtual data" can also be covered. On the other hand, data protection law addresses 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; 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.

Conceptualized within the framework tailored to social contexts and legal perspectives, information involves meaning. Pieces of information are elements of meaning that may base on data (or on observations or communications) and are then created by interpretations which take place in a particular social context.[146] 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 and for a description of the object to be regulated. In the structural dimension of such context, knowledge – founded upon texts, files, archives, registers, databases, expert systems, but also upon institutional, organizational or procedural arrangements – makes interpretation possible, and limits the possibilities of interpretation.[147] In the temporal dimension, data as well

146 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.

147 In more detail and with further references *Marion Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Voßkuhle, Eifert and Möllers (eds.), Grundlagen des Verwaltungsrechts, Vol. I, 3rd ed. 2022, § 22, Rn. 8 ff.

as information is constantly generated anew and altered during processing operations. Information and knowledge 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 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, actions and decisions is in the focused context.

As a result, data must be conceived of within a network of several fundamental elements: information, communication, knowledge, decisions and actions. It is one, but not the only reference point. Data protection law aims at regulating data processing, but precisely also at regulating the generation of information and knowledge, at influencing the decisions based on such generation, and at preventing adverse consequences for the individuals affected. At the same time, these analyses show at what fundamental level we are working when regulating data and information. It is as fundamental as regulating decisions or actions.

II. Essentials of appropriate legal approaches

With this subject matter in mind, we can already reach some insights: 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 is obvious. The characteristics of the subject matter also point to the necessity of partly novel doctrinal approaches and of elaborating complex relationships between constitutional provisions and statutory law. Data protection interests are to a certain extent in need of being concretized and shaped by law.

1. Multi-layered, multi-dimensional and multifaceted guarantees and rights

Firstly, constitutional guarantees and rights must be developed within a multilayered framework. At first sight, the factual fundamentals suggest an extension of the concept of freedom anchored in each fundamental right to the handling of data and information. 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 Court of Justice mentions the freedom of expression quite regularly. The freedom of assembly has been acknowledged as being relevant in 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 in particular contexts are considered, the application of 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-oriented, and aims at avoiding harms beforehand in a way that "we cannot afford to wait to vindicate it only after it has been violated"[148], we must be able to describe, 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. But the problem can be solved by distinguishing two or more levels on which the constitutional requirements are to be developed. Meeting 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

148 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."

more concrete protection interests that emerge in particular contexts may be covered by the guarantees of the specific fundamental rights.

Secondly, 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 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.

Thirdly, 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 data and information 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 behavior 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 processing of personal data and information. From a general perspective, i.e. leaving aside the special cases, personal data cannot be assigned to the person in question like an object belonging to him or her. Individualistic patterns of assignment fall short. 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 conceptualized with regard

to the sociality of the individual and to structurally involved counterparts. Hence, they require their own separate patterns of description.

2. 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 defense against encroachments have dysfunctional prerequisites and limitations.[149] 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 often falls short of what is needed. Protection of personal data has to base upon the further development of the functions and the contents of fundamental rights.

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 recognized in many countries by now. Modern codifications reflect the diversity of dimensions of protection in their catalogs 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 state to provide a regulatory framework and to protect individuals through legal rules and actions. 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.

3. Interplay between fundamental rights and statutory regulation

One of the core questions of all interpretations of fundamental rights that go beyond the "classical" defense against encroachment is the problem of the extent to which it is possible to develop provisions that are sufficiently clear to be effective as constitutionally binding from the textually relatively

149 More closely *Marion Albers*, Realizing the Complexity of Data Protection, in: Gutwirth/Leenes/de Hert (eds.), Reloading Data Protection. Multidisciplinary Insights and Conteporary Challenges, 2014, 213 (216 f.).

vague fundamental rights. 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 an appropriate legal framework at a basic level. Under these circumstances, the pertinent fundamental rights must be interpreted as provisions that are directed at requiring legislation to achieve certain goals and fulfill 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 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 challenges can be handled if we understand the pertinent fundamental rights in such a way that they take into account 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. 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 press, and, above all, of the freedom of broadcasting.[150] As a result of such a process of interpreting, 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

150 See, for example, the landmark judgment *FRAG* of 1981, Decisions of the FCC, Vol. 57, 295, 319 ff. Initially, the fundamental right that safeguards broadcasting freedom provides merely general requirements, but no particular model of how to regulate and organize 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.

and evolution"[151]. However, the relation is neither reverse nor is it a circle. It is important to note that the relative hierarchy between fundamental rights requirements and legal regulations always continues to exist. The underlying image may be that of a spiral with relative hierarchies, i.e. hierarchies that are constantly being re-constituted at each of the different stages. Altogether, the interplay between fundamental rights and statutory regulations in the field of data protection becomes extremely challenging.

III. Concretizing protected interests within a multi-layered conception

All in all, data protection responds to threats to freedom and needs for protection that require their own separate patterns of description, must be located at different levels and are manifold and diverse. An approach to fundamental rights that is in line with our insights calls for developing a complex bundle of provisions and rights within the framework of a multi-layered conception. This bundle must be open to ongoing revision and constantly adapted to novel threats.

1. Basic level: 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 1960s and have increased even further with the internet. In a rough summary, the crucial problems center around a potentially all-encompassing, unlimited and non-transparent processing of personal data and information by the state or other private parties. 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-centered works, more recent novels, such as Dave Eggers' "The Circle", might be added with a view to social networks. 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

151 *Yordanka Ivanova*, The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World, in: Hallinan, Leenes, Gutwirth and De Hert, Data Protection and Artificial Intelligence, 2021, 145 (151).

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."[152] 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 problems that data protection shall countervail. Data protection provisions and rights aim at ensuring that the handling of personal information and data is not largely unbound, unlimited, intransparent, or beyond any possibilities of influencing procedures or results. In the first place, they center on requiring the establishment and implementation of a legal framework suitable for countering the fundamental threats. This already requires a very sophisticated legal framework and a wide range of legal instruments. Additionally, as we have seen, the legal framework at the basic level also has the function of ensuring that contextually definable risks which the data subjects may face are recognizable 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 contexts of data processing are limited and shaped, 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.

In the legal approaches to the content of the relevant fundamental rights requirements for regulating the handling of personal data and information, a level precedent to cases that can be contextually delineated is recognized and addressed to a certain extent. This 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.[153] This presupposes, of course, that it is understood not as individual control over personal data, but

152 *Daniel Solove*, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review 1393, 1426 (2001).

153 See for references to the democratic order Decisions of the FCC, Vol. 65, 1, 43.

as multilayered, multidimensional, and multifaceted.[154] 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.[155] However, as the right to privacy covers many facets from pre-conditions to various protected interests in contextually delimited cases 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 Art. 2(1) in conjunction with Art. 1(1), 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 fundamental rights conceptualization.[156] Even better suited to such an approach is a right of individuals "to" the "protection" of personal data concerning them. 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 Art. 8(1) CFR, these considerations are consistent with the fact that Art. 8(2) and (3) CFR lays 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. Art. 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

154 Cf. also, from an overarching point of view, *Paul de Hert* and *Cristina 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, 2024.

155 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*, Part R (p. 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.

156 *Albers* (n 106), 454 ff.

above, are met through appropriate regulation. This is not done with *any* regulation. In particular, 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.[157] As explained above, in the interplay of fundamental rights and statutory regulations, the provisions of the right to the protection of personal data need to be continuously reapplied at more specific levels with more concrete requirements.

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. It sets the stage for them to enter the scene.

2. Second level: Data protection rights from specific fundamental rights

At a second level, 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 concretize fundamental rights requirements. The jurisprudence of the courts, as shown, has in principle recognized the relevance of the specific fundamental rights.[158] However, specific freedoms are often mentioned

157 Cf. *Albers* (n 149), 229 ff. Cf. also with partly different considerations, *Nikolaus Marsch*, Das europäische Datenschutzgrundrecht, 2018, 127 ff.; *Lorenzo Dalla Corte*, A right to a rule: On the substance and essence of the fundamental right to personal data protection, in: Hallinan, Leenes, Gutwirth and De Hert (eds.), Data protection and privacy: Data protection and democracy, 2020, 27 (38 ff.).

158 See n 74, 75, 80, 95.

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 then can 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 contextually specific harms and 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-oriented way from a supraindividual perspective, keeping in mind the characteristics of data, information, and knowledge. Provisions and individual rights can be applied exactly where and insofar 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.

3. 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. At the same time, it becomes clear, that it is necessary, but also possible, to embed data protection rights in overarching contexts and to coordinate them appropriately with other legal regimes.

E. Conclusion and Outlook: Data Protection as an Integral Part of the EU Data and Digital Strategy

Protection of personal data does not encompass a uniform legally protected good. In particular, the idea of control over one's own data fails because it does not fit the subject matter to be protected. Instead, protection of

personal data points to a variety of protected interests and to a bundle of provisions and rights that has to be developed in the framework of a multi-level approach as a functional cooperation of coordinated fundamental rights.

Data protection places high demands on law. 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-oriented, they are and should be only a small component of a much larger architecture.[159] The statutory rules and the 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 utilize the entire spectrum of legal forms and instruments. 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 legislation competences, in the use of legal terms which are vague and need to be concretized, 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. Regulatory concepts are therefore complex on its own terms and in addition, they have to be interwoven. The emerging variety of regulatory concepts is also compatible with a less legislation-centered understanding of law and regulation. From a political-science point of view, it has been analyzed, 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, data subjects. An appropriate normative conception has to be responsive to the interplay of actors generating and concretizing 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.

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

159 *Daniel Solove*, The Limitations of Privacy Rights, 98 Notre Dame Law Review 975, 977 ff. (2023).

between the rules of these regimes and data protection law is increasingly evident, and this is a very challenging task.[160] 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 to some extent sticks to traditional patterns of data protection that are not compatible with some of the other regulatory concepts, it cannot remain untouched. As a prerequisite, the fundamental rights and protected interests of data subjects must also be rethought and reconceptualized.

160 See *Anna Schimke*, Forgetting as a Social Concept. Contextualizing the Right to Be Forgotten, in: Albers and Sarlet (n 2), 179 (190 ff.).