Serge Gutwirth • Ronald Leenes • Paul De Hert
Editors

Reloading Data Protection

Multidisciplinary Insights and Contemporary Challenges

Editors
Serge Gutwirth
Law, Science, Technology
and Society (LSTS)
Faculty of Law and Criminology
Vrije Universiteit Brussel
Brussels, Belgium

Paul De Hert
Law, Science, Technology
and Society (LSTS)
Faculty of Law and Criminology
Vrije Universiteit Brussel
Brussels, Belgium

Ronald Leenes
Tilburg Institute for Law, Technology
and Society (TILT)
Tilburg University
Tilburg, Netherlands

ISBN 978-94-007-7539-8 ISBN 978-94-007-7540-4 (eBook)
DOI 10.1007/978-94-007-7540-4
Springer Dordrecht Heidelberg London New York

Library of Congress Control Number: 2013947601

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Chapter 11
Realizing the Complexity of Data Protection

Marion Albers

11.1 Introduction

Realizing the Complexity of Data Protection sounds a bit off-putting. Would it not be a better approach to lay down a few simple principles that would provide legal guidance for processing personal data? In contrast to such thinking, the present contribution advances the thesis that data protection is by its nature an extraordinarily complex field and therefore requires multi-level and complex regulation. Yet at its core, the legal framework is still characterized by out-dated concepts going back to when data protection first emerged. This applies both to the understanding of fundamental rights relevant to data protection and to the basic approaches to regulation. Modern data protection calls for new legal approaches.

The article provides a legal analysis both of the influential legal intellectual approaches and of the central legal provisions and also identifies areas where reconceptualizations are needed. Other analyses of legal rules would be equally interesting: for example, from a political-science perspective concerning the impact of lobbyism or from an engineering perspective regarding the transformation of data protection into technological concepts. However, the legal perspective, which addresses the understanding of legal rules in terms of legal theory, doctrinal constructions and methodological approaches, is just as important for data protection. After all, the law substantially shapes data protection by means of patterns that can be explained in a manner intrinsic to the legal system. Yet every sophisticated legal approach is also characterized by the fact that it is able to incorporate insights from other disciplines, that is, to guarantee that the law is appropriately receptive and that it is compatible with concepts across various disciplines. Precisely this is what data protection law must be able to achieve, as data protection lies at the intersection of numerous disciplines. This is another reason why sufficiently complex regulatory concepts are necessary.

M. Albers (✉)
Fakultät für Rechtswissenschaft, Universität Hamburg, Rothenbaumchaussee 33,
20146 Hamburg, Germany
e-mail: marion.albers@uni.hamburg.de

S. Gutwirth et al. (eds.), *Reloading Data Protection*,
DOI 10.1007/978-94-007-7540-4_11, © Springer Science+Business Media Dordrecht 2014

Legally speaking, data protection is characterized both by fundamental rights and by legal principles and provisions. The norms cannot be understood by examining only their wording. More important are the concepts underpinning them that guide the understanding of the norms. The present article analyzes them less from the perspective of legal method, which involves the interpretation of certain rules in a way that is consistent with the method, but more from a legal-theory and doctrinal perspective. The deliberations center on German and European law. They put German law into focus as a continental European legal system oriented toward codification in which data protection law was developed fairly early and has in the meantime been elaborated to become an extensive complex of norms addressing fundamental rights as well as legal rules. An impact on European law arises from reciprocal influences in law-making and from the network of jurisdiction among the German Federal Constitutional Court, the European Court for Human Rights, and the European Court of Justice.

The analysis starts by presenting the conception of fundamental rights (Sect. 2.1) as well as of protected interests (Sect. 2.2). Beyond the right to privacy, the right to informational self-determination has become a guiding principle, especially in the German legal system. Sect. 3 demonstrates to what a large extent the concepts of fundamental rights influence the approaches, principles and legal constructs of data protection law. My hypothesis is that the elementary patterns of thinking must be constructed in a different way in order to achieve appropriate data protection law. Data protection will then prove to be a highly complex and novel field involving particular challenges for law. This hypothesis shall be explained in Sect. 4 with three aspects in mind: Firstly, the object of data protection is complex, namely not only personal data, but a network consisting of several basic elements: data and information, knowledge and the flow of data and information, decisions and the consequences of decisions (Sect. 4.1). Secondly, data protection cannot be reduced to a uniform legally protected good. It encompasses a complex bundle of interests and legal positions aiming at protecting the individual in his or her sociality (Sect. 4.2). Thirdly, data protection requires complex concepts of regulation that must not only coordinate data protection law with the issue-related substantive legal norms appropriately, but must also take up basic elements of risk regulation or technology law (Sect. 4.3). After all, data protection law is anything but bureaucratic. It is modern and exciting, and at the same time requires additional elaboration in many respects.

11.2 Guiding Paradigms of Data Protection Based in Fundamental Rights

The concept of data protection emerged in the 1970s against the background of central mainframe computing systems. At the European level as well as in Germany the first sets of legal rules were developed.[1] With huge amounts of data being processed in these systems in a predefined sequence, the idea was that the individual steps of

[1] See the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981; Mayer-Schönberger 1997, 219, 220 ff.; Bygrave 2002, 94 ff. As

data processing, including data collection, data storage, and data use, would have to be controlled. Attention was focused on regulating the individual steps of data processing.[2]

This background and the patterns of thinking associated with it not only formed the basis for early data protection rules, but also for the substance of fundamental rights which were concretized or developed in response to the challenges processing personal data electronically. Starting in the 1970s, the right to privacy began to be interpreted in a new way.[3] In Germany, the Federal Constitutional Court derived the right to informational self-determination in its 1983 decision concerning the census ("Volkszählungsurteil").[4] Later, fundamental rights quickly became the guiding principles for the general understanding of data protection by law.

For their part, fundamental rights are linked to certain patterns of observation and thinking. The traditional understanding of fundamental rights is connected to liberal paradigms. According to this notion, fundamental rights are about protection against encroachments by the state. Although extensions of the functions of the fundamental rights, e.g., rights to protection by the state or institutional guarantees, are recognized in principle by now protection against encroachments is often considered the primary dimension of protection in fundamental rights; it still is the leading approach. However, this approach has prerequisites and limitations influencing the substance and the functions fundamental rights can have. The newly derived right to informational self-determination can illustrate this very clearly. In the following section, the traditional concept of fundamental rights and its limitations will be elucidated as well as the characteristics of the right to informational self-determination.

11.2.1 The Traditional Concept of Fundamental Rights

11.2.1.1 Protection Against Encroachments as a Central Pattern of Fundamental Rights

According to the "classical" view based on liberalism, fundamental rights serve primarily as protective rights of the individual against interventions by the state.[5] The persons protected enjoy certain freedoms or legal positions. State measures interfering in these freedoms can be fended off by means of legal remedies, provided they are not covered by constitutional law.

---

to the modernization see www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp. See also Nouwt 2009, 275, 286 ff. For data protection history in Germany see Abel 2003, Chap. 2.7 Rz. 1 ff.; Simitis 2011, Rn. 1 ff.

[2] Influential in Germany: Wilhelm Steinmüller/Bernd Lutterbeck/Christoph Mallmann/Uwe Harbort/Gerhard Kolb/Jochen Schneider, *Grundfragen des Datenschutzes*: Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BTDrucks. VI/3826, Anl. 1.

[3] See, among others, Westin 1970, p. 42.

[4] BVerfGE 65, 1, 42 ff.; Dec 15, 1983, Census Judgment.

[5] Negative liberty, see i. e. Berlin 1969, 118 ff. With regard to the jurisdiction of the FCC see BVerfGE 7, 198, 204 f.—Lüth—68, 193, 205.

The traditional view of protection against encroachments as a central pattern of fundamental rights is reflected more or less distinctly in their codification, i.e. in the European Convention on Human Rights (ECHR), in the Charter of Fundamental Rights of the European Union (Charter) or in the German Basic Law (Grundgesetz: GG). The jurisdiction of the European Court of Human Rights, of the European Court of Justice and of the German Federal Constitutional Court has elaborated the function of the fundamental rights to protect against encroachment in numerous decisions.

In terms of their structure, fundamental rights involve on the one hand the scope of protection and—on the other—the reservation allowing legal regulation provided that such regulation meets all constitutional requirements. For example, their scope of protection safeguards the right to respect for private life or the free development of one's personality[6], freedom of expression[7], and the inviolability of the secrecy of telecommunications.[8] The crucial point is that the classical concept takes these freedoms as a given. The role of the state is reduced to the function of limiting freedom with regard to public good or the rights of others. The reservations included in fundamental rights allocate this task primarily to the legislature and enables it to limit the guarantees of freedoms by means of constitutional statutory regulations.[9] All interventions by the state require a statutory basis. This basis must take the relevant constitutional requirements, especially the principle of the clarity and certainty of provisions and the principle of proportionality, into account as must the executive branch in any decision founded upon that statutory basis.

11.2.1.2 Limitations of the Concept

The understanding of fundamental rights as protection against encroachments on rights seems to be a far-reaching, optimal protection of freedom. But in fact, it has

---

[6] Article 8 (1) ECHR: "Everyone has the right to respect for his private and family life, his home and his correspondence."; Article 7 EU Charter: "Everyone has the right to respect for his or her private and family life, home and communications."; Article 2 (1) GG: "Everybody has the right to the free development of his or her personality [...]".

[7] Article 5 (1) GG: "Everyone has the right freely to express and disseminate his or her opinions in speech, writing and pictures [...]".

[8] Art. 10 (1) GG: "The secrecy of communication by letters and of telecommunication is inviolable."

[9] See Article 8 (2) ECHR: "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."; Article 52 (1) EU Charter: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."; Article 2 (1) GG: "[...] provided that they do not interfere with the rights of others or violate the constitutional order or moral law." or Article 5 (2) GG: "These rights shall be subject to the limitations laid down by the provisions of the general laws and to statutory provisions for the protection of young people and to the obligation to respect personal honour."

many prerequisites and is accompanied by limitations due to its structure. As the traditional concept of protection against encroachments builds on liberal conceptions of fundamental rights, "freedom" is understood as a pre- or non-state sphere, i.e. as a sphere antecedent to the state or external to it, and as "natural freedom."[10] Consequently, fundamental rights are directed solely toward the protection of freedoms that already exist. The social preconditions of individual freedom or, expressed more radically and more precisely, the social foundation and embeddedness of individual freedom are not given consideration. The approach also results in specific subject matters or interests which are to be protected by fundamental rights. They are conceived of as individualistic, i.e. from a perspective focusing on the individual and in the form of an individual good that is not already structurally limited.[11] Protection is granted, in particular, to individual self-determination, to individual decisions and behavior at will, to one's own body, or to property.

In liberal thought on fundamental rights, the state appears exclusively as an institution that limits individual possibilities to decide or to act freely. Such limitations must be justified, namely by the parliament passing a law that pursues a legitimate goal, that is as precise as possible both in its legal requirements and its legal consequences, and that is commensurate with the principle of proportionality. Such laws guide and limit the decisions of the executive. Just as the concept of freedom and the scope of protection of individual rights are shaped in specific ways, the role of laws and the requirements of the design of laws are tailored exclusively toward justifying limitations on freedom. The multi-dimensional role of the legislation as well as of laws is disregarded.

11.2.2 Informational Self-Determination as a Protected Interest

The classical-liberal concept of fundamental rights also characterizes the form in which the goods to be protected by data protection are described. This applies especially clearly to the right to informational self-determination. This right is the decisive fundamental right in the realm of data protection in Germany. However, it is also being mentioned with greater frequency in the transnational and European debate as a central right worthy of protection.[12] Several scholarly debates are about how to understand or how to concretize this right. This section analyzes the right to informational self-determination with a view to the influential jurisdiction of the German Federal Constitutional Court, which has developed and established it. At least in this respect, the construction of this right and the description of its scope of protection are based upon traditional doctrinal concepts and are therefore insufficient.

---

[10] Böckenförde 1974, 1529, 1532; Lühbe-Wolff 1988, 75 ff.

[11] Alhers 2005, 30 ff.

[12] See, i.e., Schwartz 1989, 675 (677 ff., 701). See also Raab and Goold 2011, 17. With distinguishing considerations Rouvroy and Poullet. (Fn. 1), 45, 52 ff. For an overview of the constitutional rights in European countries see Leenes et al. 2008.

The Federal Constitutional Court derived the right to informational self-determination from the general right of personality guaranteed by Art. 2 in conjunction with Art. 1 GG[13] in its 1983 decision concerning the census.[14] The right to informational self-determination confers on the individual the power to, in principle, determine for himself or herself the disclosure and use of his or her personal data.[15] Individuals have the right to decide themselves whether and how their personal data is to be divulged 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 he protected called "informational self-determination"? Its precursor is the right to privacy, which is also anchored in Art. 2 in conjunction with Art. 1 GG and was recognised in the case-law of the Federal Constitutional Court since the 1970s. The Federal Constitutional Court originally conceived this right employing the spatial imagery of areas of retreat walled off from the outside world, or similarly isolated situations for interaction and communication, and as the right to be let alone, or as the right to keep events in this isolated sphere confidential.[16] The right to privacy centered on a spatially as well as thematically specified area which is to remain, in principle, free of undesired inspection. This was the traditional, narrow concept of privacy. This concept drew the same broad criticism as it did in the 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.[17] 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 couched this idea in these terms as early as 1972.[18] 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 emerge but rather about which information could be derived from data obtained and how that information could be used.[19] In other words, what is decisive is not the context data originate from but rather the context in which the information is used. The Federal Constitutional Court responded to these central points of criticism of the rather narrow concept of the right to privacy understood as a protected sphere by developing the idea of a right to informational self-determination

[13] 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."

[14] BVerfGE 65, 1, 42 ff.; Dec 15, 1983, Census Judgment. Subsequent decisions are, amongst others, BVerfGE 78, 77, 84 ff.; 84, 192, 194 ff.; 113, 29, 46 ff.; 115, 166, 188 ff.

[15] BVerfGE 65, 1, 43. Analyzing the decision and its background: Albers (Fn. 11), 149 ff.; see also Rouvroy and Poullet (Fn. 12), 52 ff.

[16] BVerfGE 27, 1, 6 ff; 27, 344, 350 ff.; 32, 373, 378 ff.; 33, p. 367 376 ff.; 44, 353, 372 ff. See also Warren and Brandeis 1890, 193–220.

[17] See Schlink 1986, 233, 242; Solove 2004, 212 f.

[18] Westin 1970, 42.

[19] See Simitis 1971, 673, 680.

which centers on individual decision capacities as well as on the context of use.[20] The Court 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 a person is unsure whether deviating behaviors may be stored as information and used to his/her disadvantage, he/she will try not to attract attention by such behavior and is no longer free to act at will.[21] That is why the protection of fundamental rights must cover the protection against information and data processing by the state. The Federal Constitutional Court then shaped this extent of protection with reference to freedom of decision and action. Just as people can decide about their actions, they also have the right to determine how "their" personal data will be processed.

What characterizes this right to informational self-determination? It reaches beyond the classical understanding of the right to privacy. Its core element is a relatively abstract and therefore far-reaching individual right to make decisions ranging from disclosure of data to their processing and to their use. Even if the right to informational self-determination is derived from the right to the free development of his or her personality and from human dignity[22], its scope of protection is shaped likewise a property right.[23] Similar to some American conceptions of privacy—"Privacy," *Charles Fried* writes, "is the *control* we have over information about ourselves [. . .], is control over knowledge about oneself."[24]—informational self-determination is thought of as a right of control over personal data. The holders of fundamental rights also have the right to know by whom and for what purposes personal data referring to them are processed[25], but that right is accessory in the context of the concept.

The fundamental right protects this right to decide over the disclosure, processing and use of personal data as an individual protection against any encroachment. It follows from such a scope of protection that, as a matter of principle, every step in processing personal data is to be considered as an encroachment on the right to informational self-determination. Therefore, every step in processing personal data must be based either on consent or—more important[26]—on a constitutional legal basis which has to meet the requirements of the principles of clarity and

---

[20] For literary sources of the Court's decision see Hermann Heußner (former judge at the FCC preparing the Census Decision), 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) 1974, 23 (32).

[21] BVerfGE 65, 1, 43.

[22] See the considerations of Rouvroy/Poullet (Fn. 12), 52 ff.

[23] It is true that the FCC also stated: "The individual does not have a right in the sense of an absolute, unlimitable mastery over 'his' or 'her' data; he/she is rather a personality that develops within a social community and is dependent upon communication.", BVerfGE 65, 1, 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.

[24] Fried 1968, 475, 482.

[25] BVerfGE 65, 1, 46.

[26] The core of the right to informational self-determination is not that consent has to play a key role. Theoretically and practically more important is that a constitutional legal basis is necessary to justify data processing.

determinedness and of proportionality.[27] Additionally, the Federal Constitutional Court emphasized the principle of specifying the purposes of data processing in advance and the principle that further data processing is bound to the original purpose.[28] These consequences already show the far-reaching influence such a concept of informational self-determination has on data protection laws.

11.3 Influence on Data Protection Approaches and Principles

In Germany, the right to informational self-determination is very firmly entrenched and has many ramifications and marks the approaches, principles, legal constructs and laws pertaining to data protection to this day. The respective patterns of thinking have also influenced the Data Protection Directive of the European Union and the fundamental right expressed in Art. 8 of the EU Charter of Fundamental Rights via reciprocal influences in law-making. Similarly, they affect court rulings via the network of jurisdiction among the German Federal Constitutional Court, the European Court for Human Rights, and the European Court of Justice.[29] In this section, important implications these patterns of thinking have on the approaches, principles, and legal constructs of data protection are highlighted.

Informational self-determination, shaped as the individual right to decide over the disclosure, processing and use of personal data, centers on data, specifically the individual piece of personal data, and in the broader sense its processing in a sequence of pre-defined steps—collection, storage, alteration, use, transfer. Additionally, "data" and "information" are treated as though they were synonyms. This reflects an ontic concept of information, namely the idea that information is a kind of depiction of reality and that data could be treated as if they were objects. Views of this kind occur in the basic approaches and in the legal definitions of data protection law. For example, the German Federal Data Protection Act (Bundesdatenschutzgesetz: BDSG) does not distinguish between data and information (§ 3 I BDSG) and focuses on the lawfulness of the collection, storage, use or transfer of personal data (§§ 4, 13 ff., 27 ff. BDSG). Similarly, both the Directive 95/46/EC[30] and the Proposal of the Commission for a General Data Protection Regulation[31] define personal data as any information relating to an identified or identifiabe natural person or data subject

[27] BVerfGE 65, 1, 44 ff.

[28] BVerfGE 65, 1, 46.

[29] For Data Protection in the Case Law of the EctHR and the ECJ see de Hert and Gutwirth, (Fn. 1), 3, 14 ff.; Siemen 2006, p. 51; Schweizer 2009, 462, 464 ff.

[30] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281/31.

[31] Proposal of the European Commission of 25 January 2012 for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final.

(Art. 2 of Directive 95/46/EC; Art. 4 GDPR-Proposal) and lay down conditions under which the processing of data, defined as any operation or set of operations which is performed upon personal data, is lawful (Art. 2, 5 ff. of Directive 95/46/EC; Art. 2, 5 ff. GDPR-Proposal).

It is only owing to this ontic concept of information and data that the protected interest can he formulated analogously to the concept of property, namely as the right of disposal over processing of personal data carried out by others. The idea of informational self-determination as the exercise of individual control over data or information can be found throughout data protection law.

As the individual's authority to decide about any processing of personal data is protected, every step in processing personal data requires either consent or a legal basis. Both German and European data protection law include the principle that, apart from their legitimate use with a person's consent, personal data must not be processed in the absence of a legal basis (§ 4 I BDSG, Art. 8 II 1 EU Charter, Art. 7 of Directive 95/46/EC). This basis has to permit, in sufficiently precise form, such processing for legitimate purposes. Explicit purposes are to be specified for data processing in advance (§§ 4 III, 13, 14 I, 15 I, 16 I BDSG; Art. 8 II 1 EU Charter, Art. 6 (b) of Directive 95/46/EC, Art. 5 (b) GDPR-Proposal). Further data processing is principally hound to these purposes or at least may not be incompatible with these purposes (§§ 14 I, II, 15 I, III, 16 I, IV BDSG; Art. 6 (h) of Directive 95/46/EC, Art. 5 (b) GDPR-Proposal).[32] The entire approach is guided by the idea that courses of action and decision-making processes could he almost completely foreseen, planned and steered by legal means. In Germany, this has resulted in a far-reaching juridification and in a multitude of data protection laws, which, however, often simply map the data processing steps.

11.4 The Complexity of Data Protection: Analyses and Consequences

Data protection law has been in flux for some time now. Changes in basic societal and technical conditions have often been pointed out. But the issue is by no means simply one of adaptation to changes in external conditions. At a fundamental level, the patterns of thought and description used in data protection law must be reflected upon critically and reconceptualized.

This shall be explained for three points in particular: firstly, for the subject matter at hand; secondly, for the description of the protected interests; and thirdly, for the

[32] The requirement that personal data must not be further processed in a way incompatible with the specified purposes sets lower standards than the requirement that further data processing is principally bound to the purposes specified in advance. Additionally, the meaning of "incompatible" requires interpretation. See for the functions of the principle of specifying purposes and of binding data processing to the purposes specified in advance Albers (Fn. 11), 168 f., 498 ff.

concepts for regulation. As a result, it will emerge that in all respects data protection requires an innovative approach, is highly complex, and poses unprecedented challenges for law.

11.4.1 The Complexity of the Subject Matter: Data and Information, Knowledge and Flow of Data and Information, Decisions and Consequences of Decisions

The goal of data protection is not the protection of data but of the individuals to whom the data refer. The object of protection, then, is not the personal data per se. We must expand this isolated view by including several 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.

Concepts of "data" and "information" are described in multifarious and discipline-dependent ways.[33] In the (social) context of data protection it is at least important to realize that data and information are not synonymous. On the contrary, they must be strictly differentiated. Data might be described as characters recorded 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 characterized by the various media, technologies, and networks.[34] Due to their objectification, data can be conceived of distinctly and provide a starting point for legal regulation. Nonetheless, data are not meaningful per se, but rather as "potential information". Their information content is not an intrinsic attribute of the data themselves.[35] It is created only by means of interpretation in the particular context of interpretation.

Information involves meaning, and pieces of information are elements of meaning. Units of information may base on data (or on observations or communications) but data only attain meaning by being explained and interpreted by the recipient or data user who uses data to obtain information. Devising meaning depends on the individual situational conditions for interpretation as well as on the context of the knowledge and interpretation.[36] 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.

---

[33] See, for example, Floridi 2010, 19 ff.

[34] See, among others, Waldo et al. 2007, 88 ff.

[35] See with regard to communication Ashby 1963, 124: "The information conveyed is not an intrinsic property of the individual message."

[36] Albers 2002, 61, 67 ff. See also Bateson 1972, 315 ff.

Due to the fact that information requires interpretation, which takes place in a particular context of knowledge and interpretation and is dependent on the individual, situational conditions of interpretation, information refers to the structures and processes within which it can be created in the first place. In the structural dimension, knowledge is involved in generating information. Knowledge is founded upon texts, files, archives, registers, databases, expert systems, but also upon institutional, organizational or procedural arrangements. It makes interpretation possible, and limits the possibilities of interpretation. Knowledge is a factor and a product of the context in which handling of information and data occurs and it influences this handling inherently.[37] Whether or not data processing poses risks to the person the data refer to also depends on the knowledge that exists or can be developed in a particular context or in a particular case. That is why data protection must also take the knowledge level into account.[38] In the temporal dimension, the procedural character of data processing comes into play as well. Data and information are constantly generated anew and altered during processing operations. In addition, a collection of personal data reveals its social and legal meaning only when one views it along with its linkages to other data, its use, or its transfer to other agencies. For example, one can understand what it means if personal telecommunications data is stored longer than necessary for billing (in the context of data retention)[39] only with the duties of telecommunications companies in mind to transmit personal data to the security authorities which then use the data for further investigations against the respective person.[40]

The ways in which data and information are handled, the knowledge and the processing operations are impacted by the media, technologies, and networks employed. Whether data are stored in paper files, automated electronic files, or in network systems has an influence on, for instance, the quantity and the form of data that can be stored and easily accessed, the potentials for interlinking them, or the possibilities for transmitting data. Media, technologies, and networks can increase the dangers individuals are subject to, but can certainly also limit such vulnerability by putting technical barriers and safeguards related to data processing into place.

What matters not least is the connections between information or knowledge on the one hand and the decisions made by the public or private bodies processing the data on the other. In the end, information and knowledge serve as bases for certain decisions and actions. Such decisions have consequences. They may have an adverse effect on the person to whom the data and information refer in the form of a limitation of his/her freedom. And protection from unjustified disadvantages is one of the reasons for data protection.

---

[37] Albers 2012, § 22 Rn. 14 ff.; Trute 2010, 11 ff.

[38] See also Mireille Hildebrandt, *Who is Profiling Who? Invisible Visibility*, in: Gutwirth et. al. (Fn. 1), 239, 240 ff.

[39] Article 3 of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks [...], Official Journal L 105/54.

[40] See BVerfGE 125, 260 (318 ff.). For a critical review of this Decision see de Vries et al. 2011, 3 ff.

As a result, data protection deals with highly complex subject matter: It is necessary to operate with the differentiation between data and information. The dimension of knowledge and the temporal dimension of data and information flow must be regarded as well as the decisions and consequences of decisions. In other words, any new concept would be misguided if it just focused on information rather than on data, and simply substituted one term for the other. On the contrary, data remains an important reference point for legal regulation. But data must be conceived of within a network of several fundamental elements and is not the only reference point. Data protection 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.

11.4.2 The Complexity of the Protected Interests of Affected Individuals

This brings us to the second point: How can we describe the protected interests of affected individuals? At the center of the legal discussion are a few very abstractly stated descriptions of legally protected goods which are related to fundamental rights: Private life or privacy[41], protection of personal data, informational self-determination. Art. 8 ECHR, the right to respect for private life[42], has been concretized to various claims against collection and storage of personal data or claims to be informed about data that refer to oneself. However, legal rulings of the European Court of Human Rights (ECtHR) unfold from case to case; the contents of what constitutes the right to respect for "private life" as a legally protected good is compiled merely casuistically.[43] Looking at Art. 7 of the EU Charter[44], Art. 16 (1) of the TFEU and Art. 8 (1) of the EU Charter[45] the right to respect for "private life" and the right to the "protection of personal data"—each one a very abstractly formulated legally protected good—stand side by side. To date, the European Court of Justice avoids a clear cut differentiation[46] and only specifically describes objectives of protection and legally

[41] For an analysis of the concept of „information privacy" in the UK see Raab and Goold (Fn. 12).

[42] See Fn. 6.

[43] See the references in Fn. 29.

[44] See Fn. 6.

[45] Art. 8 (1) of the EU Charter: "(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority."

[46] See ECJ, Rs. C-92/09 u. C-93/09, *Schecke and Eifert vs. Land Hessen*, http://curia.europa.eu, §§ 45 ff. The differentiation is necessary but not easy due to the interplay between Art. 7 EU Charter in conjunction with Art. 52 (3) EU Charter, Art. 8 ECHR on the one hand and Art. 8 EU Charter on the other.

protected goods to a very limited extent. The Federal Constitutional Court focuses on the "informational self-determination" derived from Art. 2 in conjunction with Art. 1 GG as a legally protected good. Just as well, German academic approaches have long been centered on patterns of thought such as informational self-determination, authority to decide about processing of personal data, and individual control. In recent years, there has been some movement, and a new discussion regarding the rights which data protection should safeguard has commenced. One widespread criticism argues that control is simply not possible because of the factual circumstances and the conditions of the internet. But the approach taken by this criticism is not sufficiently profound. The idea of control over one's own data fails not only because it would no longer be practicable. It fails because it does not fit the subject matter to be protected. A reconceptualization is needed which leaves the classic concept of basic rights behind. The interests which data protection is to safeguard cannot be grasped using an individualistic perspective; a multidimensional understanding of fundamental rights is required; and as a result, data protection includes a bundle of rights which must be described in a new way.

11.4.2.1 From Individualistic Patterns to the Protection of the Individual in Sociality

Protection of fundamental rights in terms of the way government agencies or other private parties handle personal information and data is different from the legally protected good in the traditional understanding of fundamental rights. It is true that a holder of fundamental rights exists. But the object of protection is not the holder's freedom of decision or of action, which would be impaired by state intervention. Instead—as the analysis of the subject matter has just demonstrated—the holder is to be protected in terms of personal information and data, which are generated and processed by others in particular contexts. Government agencies or other private bodies are structurally involved in this, due to the mere fact that data and information must be interpreted. Personal information or data cannot be assigned to the person in question like an object belonging to him or her.[47] Individualistic patterns of assignment fall short.

Reasoning why and to what extent the person in question is to be protected must rather stem from a supraindividual perspective, namely by taking a categorizing view of the context and of adverse consequences that are to be expected with regard to the person to whom data, information and knowledge refer. The fact alone that a piece of data refers to a person does not yet predicate a person's need for protection. The need for protection arises in particular in relation to negative effects of handling the personal data and the information gained from it. Legally protected goods and encroaching mechanisms require their own separate patterns of description. In addition, protection directed solely at defending against and refraining from processing personal data is insufficient. The person protected may also be interested in personal

[47] More thoroughly Allen 2000, 861, 865 ff.

data being made available so that an agency has the information at its disposal which it needs for a correct decision. And it is just as important that the person affected is informed about processing of personal data and information and can influence it. Hence, individuals need not only defensive rights, but also rights to know, to obtain information, to participate, and to exert influence. The subject matter to be protected by data protection based on fundamental rights must therefore be designed differently and be more diverse than the legally protected goods in terms of the "classical" concept of fundamental rights and the "classical" concept of protection against encroachments. Appropriate data protection requires a more sophisticated conception of fundamental rights.

11.4.2.2 The Necessity of Building Upon a Multidimensional Understanding 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 principle by now. Modern codifications, for example the EU Charter of Fundamental Rights, reflect the diversity of dimensions of protection in their catalogs of fundamental rights.[48] The German Federal Constitutional Court has derived positive obligations of the State, for example obligations to provide for the minimum income needed to exist and especially the state's duty to protect (Schutzpflicht) as well as the so-called "Drittwirkung" by which fundamental rights indirectly influence the legal relationships between private persons. Nevertheless, the court rulings of the Federal Constitutional Court, the European Court of Human Rights, and the European Court of Justice are tentative in this regard. Protection against encroachments is still considered the primary dimension of protection in fundamental rights. That is one of the reasons why, in the case of data protection, the protected interests are shaped likewise a property right. Doctrinal reasons are also evident with regard to the rather hesitant acknowledgement of fundamental rights of access to personal data[49] or of institutional guarantees. In scholarly debates, the foundations, the extent and the details of the further dimensions of fundamental rights' protection beyond the traditional understanding are the subject of heated controversy.

---

[48] See, for example, Art. 14, Art. 27 ff. EU Charter.

[49] In Germany, the first Senate Decision of the FCC which fundamentally derived rights to know not only from the guarantee to access to the courts, Art. 19 (4) GG, but from Art. 2 (1) in conjunction with Art. 1 (1) GG was not earlier than in 2008, see BVerfGE 120, 351 (362 f.); prior to that see BVerfG (Chamber Decision), NJW 2006, 1116 (1117 ff.). The ECtHR has recognised rights to access to personal files and to obtain information earlier, however, mostly in special cases, see for the rights of persons to receive the information necessary to understand their childhood and development *Gaskin vs. United Kingdom*, Judgment of 7 July 1989, Application No. 10454/83, for the right of access to health-related (not necessarily personal) data ECtHR, *McGinley and Evan vs. UK*, Judgment of 9 June 1998, Application Nos. 21825/93, 23414/94 —, Rn. 98 ff; see also ECtHR, *Segerstedt-Wiberg*, Judgment of 6 July 2006, Application No. 62332/00—, Rn. 99 ff. The Court argues cautiously: "Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in effective respect for private or family life. In determining whether or not

However, the abstract guarantees of fundamental rights are open to interpretation and permit to elaborate diverse dimensions of protection. The classical understanding is a concept which is too narrow and has dysfunctional prerequisites and limitations. Fundamental rights are not only about protection against encroachments, but also about rights to know and to obtain information, about rights to participate and to influence decisions, about rights to be protected by the state, or about institutional guarantees. As individualistic patterns of assignment and the idea of control over one's own data fall short and as the subject matter to be protected is multifarious, data protection has to base upon the further development of the functions and the contents of fundamental rights.

11.4.2.3 The Bundle of Protected Interests

"Data protection" is a rather vague concept. Some scholars emphasize that data protection simply describes the tool for safeguarding legally protected freedoms like autonomy or freedom of decision. Others assume that it points to the good or goods to be protected. It could also be understood as covering both: the means of protection and, as an umbrella term, the legally protected interests. Anyway, when it comes to the goods to be protected, data protection should not be understood as a merely instrumental concept which protects other freedoms known from the traditional concept.[50] Instead, it is necessary to leave behind the descriptions using an individualistic approach, to wit: self-determination, freedom of decision, property. The interests to be protected should be designed so that they gain their meaning when the sociality of the individual in question is taken into account. This is responsive to the subject matter elucidated above: data, information, knowledge. Hence, data protection is about protection from the creation of personality profiles, protection of a person's reputation, protection from stigmatization and discrimination, protection of normative justified expectations of privacy, protection against identity theft, protection against surveillance and protection of contextual integrity.[51] These examples illustrate that data protection does not encompass a uniform legally protected good. On the contrary, there are complex and manifold interests that are to be protected. Their wide range and contextual dependencies have already been worked out in the context of the "privacy" debates in the US, for example by Daniel Solove and Helen Nissenbaum, among others.[52]

---

such a positive obligation exists, the Court will have regard to the fair balance that has to be struck between the general interest of the community and the competing interests of the individual, or individuals, concerned [. . .]" (*McGinley and Evan vs. UK*, Judgment of 9 June 1998, Application Nos. 21825/93, 23414/94—, Rn. 98).

[50] Of another opinion: Britz 2010, 569 ff.; Poscher 2012, 178 ff.

[51] The fundamental right to the guarantee of the confidentiality and integrity of information technology systems which has been derived from Art. 2 in conjunction with Art. 1 GG by the Federal Constitutional Court in 2008—BVerfGE 120, 274—points in the right direction, but it should be understood merely as a part of data protection.

[52] Solove 2008; Nissenbaum 2008, 119 ff.; Nissenbaum 2010. See also Rössler 2001.

A closer analysis reveals that the dangers posed by processing of personal data and information and the needs for protection that data protection responds to have be identified at different levels.[53] At a basic level, the crucial problem centers on information and data processing that is all-encompassing, unlimited, and not transparent. As long as one is confronted with a situation of this kind, then no suitable estimate can be made in what contexts what information is being generated and how such information is being used or what negative consequences individuals will have to face in specific constellations. This problem of unlimited and intransparent data processing must be countered by legal regulation providing basal limits and transparency. Only on this basis is it possible to work out interests to be protected which exist in quite specific contexts due to quite specific disadvantages.

At the basic level, Orwell's "Big Brother,"[54] Bentham's "Panopticon,"[55] and Kafka's "The Trial"[56] might be illustrative as widely known, culturally anchored metaphors that—although these narratives are of course rooted in quite different contexts—take up different facets of the dangers just mentioned above. Daniel Solove has pointed out that the "Big Brother metaphor is definitely effective at capturing certain privacy problems"[57] but that it is the Kafka metaphor which captures those elements of threats to privacy which deal with certain data collection and circulation by others or other entities "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."[58] This illustrates that, at the basic level, there are already multifarious problems data protection shall countervail. Speaking legally, they are not solved by merely assigning an individual right to control personal data to the data subject. In keeping with the dangers to liberty, duties of the legislative branch and requirements of legal regulation are necessary. The legislation must regulate data processing in an appropriate way and safeguard that handling personal information and data does not take place in an unrestricted, unlimited, and intransparent way as well as it has to ensure that the individuals affected have the possibility to obtain sufficient knowledge about and sufficient influence on processing of personal data and information. At this level the state is anything but kept out.

At a second concrete level, it is about individual and specific interests to be protected, which arise for the affected person in concrete contexts in terms of adverse consequences. The capability to describe the dangers as well as the specific interests to be protected at this second level requires that basic regulation occur at the first level. An example is the problem of the domestic intelligence service monitoring a public meeting, with negative consequences for the freedom of assembly. Another example is the protection of individuals from media intrusion by publishing personal data or pictures. At this level, rights as protection against encroachments are applicable.

---

[53] See Albers (Fn. 11), 353 ff.

[54] Orwell 2008.

[55] Bentham 1995, 29 ff.

[56] Kafka 2002.

[57] Solove 2001, 1393, 1399.

[58] Solove (Fn. 57), 1426.

Nevertheless, duties to protect have to be derived, too, as well as an overall concept beyond traditional approaches is necessary.

The result shows that data protection outlines a complex bundle of interests worthy of protection. Data protection bases upon a multi-dimensional understanding of fundamental rights and requires entirely new descriptions of the protected interests: in place of legally protected goods conceived of in an individualistic way, it is about individual legal positions *in* sociality, or, in other words: the individual's social positions to be protected by fundamental rights. The bundle of protected interests and positions must still be worked out in greater detail and will also have to be dynamically adapted time and again to new dangers.

11.4.3 The Complexity of Appropriate Concepts for Regulation

The third point section of this paper shall demonstrate how complex appropriate concepts for regulation must be. To date, concepts are still characterized by the image of central mainframe computers that process data using programs in a predefined sequence. Legally, informational self-determination as the good to be protected and the reservation allowing legal regulation lead to the idea that every step in processing personal data must be justified by consent or legally regulated by means of a basis in law. But meanwhile, the pitfalls of consent are recognized as well as the multitude of laws is more and more criticized as a flood of legislation. More problematic than the quantity of laws is that the regulations often simply map the data processing steps and that the approach is characterized by the belief in planning prevalent in the last century when people were convinced that it was possible to regulate things precisely using legal means.[59]

However, fundamental rights as basis of data protection do not result in being forced to understand laws against the backdrop of their traditional role. As well as allowing the development of new legally protected goods, fundamental rights permit a multidimensional understanding of the reservations and of regulations. 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. Data protection law 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. They are therefore complex on their own terms and in addition, they have to be interwoven. Further factors make clear how challenging appropriate data protection laws are.

[59] For new challenges with regard to ubiquitous computing which affects the current principles of data protection see Čas (Fn. 1), 139, 141 ff.

11.4.3.1 A Wide Range of Regulation Elements

Rather than merely steering the steps of processing data, appropriate regulation concepts require many different elements. Regulation of data processing stages will still play an important part in the future. This form of regulation is, however, supplemented and augmented by other constituent elements: data protection through system design, data protection through the development and use of technology, organizational and procedural precautions, expanded functions of data protection officers, or quality assurance mechanisms such as data protection audits. In addition, there is a variety of affected individuals' rights to know, to obtain information, to participate and exert influence. The fact that data protection law includes a large number of constituent elements is generally recognized by now. But up to the present, elements of different origins have tended to exist side by side. In the future, they must dovetail and be interwoven appropriately. This is an ambitious task. Moreover, the constituent elements are rather complex themselves and call for highly varied instruments. This can be exemplified by data protection through system design, by data protection through technology and by individual rights to information.

Data protection through system design refers to a level preceding regulation of the steps of data processing. In summarizing broad discussions, it can be described as "data protection functionality incorporated into systems and procedures".[60] The leading idea is that regulating the steps of data processing is not sufficient because data processing takes place within certain social systems, within organizational structures and procedures and under specific technical conditions.[61] This predetermined context influences which and how many personal data is needed, how long data has to be stored, how many people have access to them and how transparent data processing is. Therefore, the legal regulation and shaping of this context prior to the subsequent processing of data and information is not less important than the regulation of the data processing operations. That makes also clear that "system design" does not refer solely to technical systems or procedures; organizational structures or decision procedures have to be taken into consideration as well.[62] Hence, data protection through system design aims at the legal shaping of the social, organizational, procedural and technical contexts in which personal data and information are handled. It has a broad scope: from the shaping of administrative competences to which data processing operations are oriented, to organizational and procedural approaches, to the technical setup of data processing equipment. Understood in this way, data protection through system design is an evidently ambitious task to fulfill. The German Federal Data Protection Act, for example, attempts to realize it by the general principle of data avoidance and data minimization (§ 3a BDSG): Systems shall be designed in a way that as few personal data are needed as possible. Whether these principles really make sense as overall principles is contested.[63] This points to

[60] Köhntopp 2001, 55, 56.

[61] See also Point 4.1 of this chapter.

[62] The scholarly elaborations are heterogeneous in this respect.

[63] More closely Albers (Fn. 37), Rn. 106 ff.

the difficulty that the realization of data protection through system design depends on a—not yet achieved[64]—clear and convincing elaboration of protection objectives and protected interests. All in all, system design as regulation element takes data protection law beyond the traditional patterns of regulatory law.

Whilst the social risks of mainframe computing systems and data processing technologies once were the reason for developing data protection concepts, technologies in the meantime are considered to be also a tool for realizing data protection. Privacy friendly or privacy enhancing technologies play an important role both in European and in national law.[65] But data protection through technology places high demands on law. The first problem is that it has to be ensured that technology with which the normative standards for the handling of personal information and data can be fulfilled is available at all. Technological developments cannot be commanded. Indirect incentives and mechanisms for exerting influence must be drawn upon, e.g. giving financial support, institutionalizing bodies or procedures for developing privacy friendly technologies or issuing quality seals and product certificates. These "soft law"-instruments might influence technology development but their influence is limited. Assumed that applicable technologies are available data protection through technology shaping defines requirements for the selection, use, and configuration of data processing networks, systems, programs, or storage media. In advance of concrete processing operations, these requirements are to ensure that normative rules are already technically established or can at least be fulfilled. Data protection through technology shaping overlaps with data protection through system design. It includes, for example, requiring data protection-friendly default settings. Data protection through the use of technology encompasses requirements of the forms of technology that accompany and secure the regulation of the steps of data processing, for instance the obligation to use encryption procedures when transmitting data. Just as data protection through system design, data protection through technology development, shaping and use is an ambitious task. And just as well, it depends on clearness about protection objectives and protected interests and, including forms of "soft law" and diverse instruments, it takes data protection law beyond the traditional patterns of regulatory law.

The rights of affected persons to information about the collection and use of personal data seem to be—although they are directed towards positive actions of the state or of private persons processing personal data—rather uncomplicated. However, they fulfill different functions: They are intended to convey to the data subjects the information they need regarding what others know about them so they can orient themselves in their social environment. They open up opportunities to participate and to influence the data and the knowledge. They safeguard the possibility of legal remedies. Due to these different functions they must be guaranteed and carried out on several levels and in a variety of forms: as general information about tasks and organizational structures of authorities or bodies processing data, as duties to

[64] See Point 4.2 of this chapter.

[65] See, i.e., Report from the Commission, First report on the implementation of the Data Protection Directive (95/46 EC), COM (2003) 265 final, 15 f.

inform or duties of notification, or as rights to access to information or to documents. Additionally, the exercise of rights to information in practice depends on social and individual prerequisites, which can be influenced only indirectly by means of law.

To conclude with another regulation element, which has to be refined: Data protection cannot be guaranteed solely by mechanisms that accord the persons affected individual protection and individual redress mechanisms. Appropriate institutional guarantee mechanisms have to be established as well[66] so that it must be decided, e. g., under which conditions they make sense and how they should be combined with individual rights and legal remedies of the data subject.

11.4.3.2 Further Characteristics of Data Protection Law

Concepts for regulation of data protection become complex not least due to the fact that data protection law must be coordinated with already existing issue-related legal norms containing, for example, tasks and competences in a particular field. A thoroughly coordination is necessary because of the close linkages between data, information, knowledge, and decisions.[67] Data protection is not a special field of law that could stand in isolation beside the substantive fields of law. Rather, data protection law pertains to a fundamental cross-cutting dimension. The need to coordinate with the substantive provisions also points to the need to differentiate within data protection law itself. For example, one must consider the questions of when sector-specific regulations are necessary, when general regulations fit best or to what extent uniform data protection law for the public and private realms makes sense.

A number of additional factors make appropriate concepts for regulation even more challenging. In contrast to the original concepts of data protection, it is in fact not possible to readily predict the handling of personal data and information, the knowledge generated from them, and the ensuing decisions. The idea that these processes could be almost completely foreseen, planned and steered by legal means[68] has turned out to be too simple. Processing of data and information, generating information and knowledge, coming to decisions on the basis of information and knowledge include dynamics and uncertainty at many points. This is all the more the case with a view to the use of technologies. Consequently, it is less the steering idea which characterizes or should characterize data protection law than, similar to environmental law, the idea of risk regulation.

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.

---

[66] More profoundly Mayer-Schönberger 2010, 1853, 1873 ff.

[67] Point 4.1 of this chapter.

[68] See Point 3. of this chapter.

Last but not least, data protection law cannot be understood against the background of the traditional ideas of hierarchical law implementation or enforcement. There are a number of general theoretical approaches aiming at superseding concepts of central steering by more flexible concepts of law. From a political-science point of view 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.[69] 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. All in all, data protection law proves to be a field of law in which new approaches are required.

11.5 Outlook: Data Protection Law as a Central New Field of Law

In sum, data protection law is a new, highly complex field of law in which a considerable amount of elaboration must still be carried out regarding its subject matter, the interests protected and appropriate concepts for regulation. Elaborating the law also depends on insights from other disciplines, for example the social sciences, the technological sciences, or information science. All this makes studying data protection law so exciting.

References

Abel, Ralf-Bernd. 2003. Geschichte des Datenschutzrechts. In *Handbuch Datenschutzrecht*, ed. Alexander Roßnagel. München: Beck (Chapter 2.7).

Albers, Marion. 2002. Information als neue Dimension im Recht. *Rechtstheorie* 33:61–89.

Albers, Marion. 2005. *Informationelle Selbstbestimmung*. Baden-Baden: Nomos.

Albers, Marion. 2012. Umgang mit personenbezogenen Informationen und Daten. In *Grundlagen des Verwaltungsrechts Vol.II, 2nd ed.*, eds. Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann, Andreas Voßkuhle. München: Beck, § 22.

Allen, Anita L. 2000. Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm, *32 Connecticut Law Review* 861–875.

Ashby, William. 1963. *An introduction to cybernetics*, 5th ed. London: Chapman & Hall.

Bateson, Gregory. 1972. *Steps to an ecology of mind. Collected essays in Anthropology, Psychiatry, Evolution, and Epistemology*. Chicago: University of Chicago Press.

Benda, Ernst. 1974. Privatsphäre und "Persönlichkeitsprofil". Ein Beitrag zur Datenschutzdiskussion. In *Menschenwürde und freiheitliche Rechtsordnung*, eds. Leibholz, Faller, Mikat, Reis. Tübingen: Mohr. 23–44.

Bennett, Colin, J., Charles, D. Raab. 2003. *The Governance of Privacy*. Aldershot: Ashgate.

Bentham, Jeremy. 1995. *The Panopticon Writings* (Edition Miran Božovič). London.

Berlin, Isaiah. 1969. Two concepts of liberty. In *Four essays on liberty*, ed. Isaiah Berlin. Oxford: Oxford University Press.

[69] See Bennett and Raab 2003; Raab 1993, 89 ff.

Böckenförde, Ernst-Wolfgang. 1974. Grundrechtstheorie und Grundrechtsinterpretation. *Neue Juristische Wochenschrift* 1529–1538.

Britz, Gabriele. 2010. Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts. In *Offene Rechtswissenschaft*, ed. Wolfgang. Hoffmann-Riem, 562–596. Tübingen: Mohr Siebeck.

Bygrave, Lee A. 2002. *Data protection law*, The Hague: Kluwer.

Čas, Johann. 2011. Ubiquitous computing, privacy and data protection: Options and limitations to reconcile the unprecedented contradictions. In *Computers, privacy and data protection: An element of choice*, ed. Serge Gutwirth, Yves Poullet, Paul de Hert and Ronald Leenes, 139–169. Dordrecht: Springer.

de Hert, Paul and Serge, Gutwirth. 2009. Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action. In *Reinventing data protection?* ed. Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwagne, Sjaak Nouwt, 3–44. Dordrecht: Springer.

de Vries, Katja, Rocco Bellanova, Paul de Hert, and Serge Gutwirth. 2011. The German constitutional court judgment on data retention: Proportionality overrides unlimited surveillance (Doesn't It?). In *Computers, privacy and data protection: an element of choice*, ed. Serge Gutwirth, Yves Poullet, Paul de Hert, and Ronald Leenes, 3–23. Dordrecht: Springer.

Floridi, Luciano. 2010. *Information. A very short introduction*, New York: Oxford University Press.

Fried, Charles. 1968. Privacy. *Yale Law Journal* 77:475–493.

Heußner, Hermann. 1984. Das informationelle Selbstbestimmungsrecht in der Rechtsprechung des Bundesverfassungsgerichts, *Die Sozialgerichtsbarkeit* (SGb). 279–285.

Kafka, Franz. 2002. *Der Proceß*. Frankfurt a. M.: S. Fischer.

Köhntopp, Marit. 2001. Datenschutz technisch sichern. In *Allianz von Medienrecht und Informationstechnik?* ed. Alexander Roßnagel, 55–66. Baden-Baden: Nomos.

Leenes, Ronald E., Bert-Jaap Koops and Paul de Hert, eds. 2008. *Constitutional rights and new technologies. A comparative study*. The Hague: Asser Press.

Lübbe-Wolff, Gertrude. 1988. *Die Grundrechte als Eingriffsabwehrrechte*. Baden-Baden: Nomos.

Mayer-Schönberger, Viktor. 1997. Generational development of data protection in Europe. In *Technology and privacy: The new landscape*, ed. Philip E. Agre, Marc Rotenberg. Cambridge: MIT Press, 219 ff.

Mayer-Schönberger, Viktor. 2010. Beyond privacy, beyond rights—toward a systems theory of information governance. *98 California Law Review* 1853–1885.

Nissenbaum, Helen. 2008. Privacy as contextual integrity. *79 Washington Law Review* 119–157.

Nissenbaum, Helen. 2010. *Privacy in context. Technology, policy, and the integrity of social life*. Stanford: Stanford University Press.

Nouwt, Sjaak. 2009. Towards a common European approach to data protection: A critical analysis of data protection perspectives of the Council of Europe and the European Union. In *Reinventing data protection?* eds. Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwagne and Sjaak Nouwt, 275–292. Dordrecht: Springer.

Orwell, George. 2008. *Nineteen Eighty-Four*. London: Penguin.

Poscher, Ralf. 2012. Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen. In *Resilienz in der offenen Gesellschaft*, eds. Hans-Helmuth Gander et al., 167–190. Baden-Baden: Nomos.

Raab, Charles. 1993. The governance of data protection. In *Modern governance: New government—society interactions*, ed. Jan Kooiman, 89–103. London: Sage.

Raab, Charles and Benjamin Goold. 2011. Protecting information privacy. *Equality and human rights commission research report series*. research report 69.

Rössler, Beate. 2001. *Der Wert des Privaten*. Frankfurt am Main: Suhrkamp.

Rouvroy, Antoinette, and Yves Poullet. 2009. The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In *Reinventing data protection?* ed. Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwagne, Sjaak Nouwt, 45–76. Dordrecht: Springer.

Schlink, Bernhard. 1986. Das Recht der informationellen Selbstbestimmung. *Der Staat* 25:233–250.

Schwartz, Paul. 1989. The computer in German and American constitutional law: Towards an American right of informational self-determination. *American Journal of Comparative Law* 37:675–701.

Schweizer, Rainer. 2009. Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zum Persönlichkeits- und Datenschutz. *Datenschutz und Datensicherheit (DuD)* 462–468.

Siemen, Birte. 2006. *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot.

Simitis, Spiros. 1971. Chancen und Gefahren der elektronischen Datenverarbeitung. *Neue Juristische Wochenschrift* 673–682.

Simitis, Spiros. 2011. Einleitung: Geschichte—Ziele—Prinzipien. In *Kommentar zum Bundesdatenschutzgesetz, 7th ed*, ed. Simitis, Baden-Baden: Nomos 2011.

Solove, Daniel. 2001. Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review* 53:1393–1462.

Solove, Daniel. 2004. *The digital person*. New York: NYU Press.

Solove, Daniel. 2008. *Understanding Privacy*. Cambridge: Harvard University Press.

Trute, Hans-Heinrich. 2010. Wissen—Einleitende Bemerkungen. In *Wissen—Zur kognitiven Dimension des Rechts, Die Verwaltung, Beiheft 9*, ed. Hans C. Röhl, 11–38.

Waldo, James, Herbert S. Lin, and Lynette I. Millett, eds. 2007. *Engaging privay and information technology in a digital age*. Washington: The National Academies Press.

Warren, Samuel D., Louis D. Brandeis. 1890. The right to privacy. *4/5 Harvard Law Review* 193–220.

Westin, Alan F. 1970. *Privacy and Freedom*. 6th. ed. New York: Atheneum.