

Informational Self-Determination: A Convincing Rationale for Data Protection Law?

by Florent Thouvenin*

Abstract: European data protection law rests on the assumption that individuals should have control of personal data about them. This control is often labelled “informational self-determination”. The idea of informational self-determination sounds convincing and promising at first. However, a closer look reveals that this idea can hardly serve as a convincing rationale for the European approach to data protection law which aims to regulate all processing of personal data by government agencies and private actors. Rather, an important distinction must be made.

Informational self-determination may well be the underlying rationale of the fundamental right to the protection of personal data as enshrined in Art. 8 of the Charter of Fundamental Rights of the European Union and it may even be qualified as a fundamental right in itself. Acknowledging such a fundamental right, however, only means that the state may not require citizens to provide information about themselves and government agencies may not use such information without a sound legal basis. But since private actors are not bound by fundamental rights, it does not entail that the relation between private actors should be based on the idea of informational self-determination. In fact, a closer look at the most important provisions of the GDPR reveals that only some of them can be based on the idea of control or

informational self-determination. Most importantly and contrary to a widespread assumption, most data processing of private actors is not based on data subjects’ consent but on the legitimate interests of the controller. The relation between data subjects and private actors, namely businesses that process personal data about their customers, is therefore hardly ever based on exercising informational self-determination. This factual finding is supported by a normative analysis which demonstrates that the idea of informational self-determination can hardly be reconciled with the principle of private autonomy and the resulting need to provide a justification for the granting of a right that allows one private actor to control the activity of another. If one acknowledges that all social interaction is based on the processing of personal data, that most individuals have little interest in exercising control of personal data about them, and that data is a public good, it is hard to find a convincing reason for the granting of a right to informational self-determination which should govern the relation between private actors. Thus, while informational self-determination may be acknowledged as a fundamental right, it cannot serve as a convincing rationale for an all-encompassing regulation of the processing of personal data by private actors.

Keywords: Informational Self-Determination; Data Protection Law; Rationale; Privacy; Protection against Harms

© 2021 Florent Thouvenin

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Florent Thouvenin, Informational Self-Determination: A Convincing Rationale for Data Protection Law?, 12 (2021) JIPITEC 246 para 1.

A. Introduction

- 1 For quite some time, data protection received little attention in law and was largely disregarded by the public. In recent years, this has fundamentally changed. The digitalisation of multiple activities and the enactment of the General Data Protection Regulation (GDPR) sparked an intense debate in academia, the media and the public. Numerous scholarly papers and newspaper articles have been published – both in law and in other disciplines. However, despite the growing interest and importance of data protection law, fundamental questions remain unanswered. Arguably the most significant one being that of the theoretical foundation of this field of law.
- 2 In Europe, surprisingly little time and effort has been devoted to investigate the theoretical foundation of data protection law and to identify a convincing rationale for the European approach which consists of an all-encompassing regulation of the processing of all personal data by government agencies and private actors¹. The lack of in-depth analysis is quite striking given that the EU introduced a fundamental right to the protection of personal data² and enacted the GDPR which is regarded the single most impor-

tant piece of regulation the EU has issued so far. As opposed to Europe, the notion and concept of privacy have been debated in the US since the publication of the seminal article of Warren and Brandeis in 1890³. While it is certainly true that privacy is a broader concept than data protection as it also covers issues such as bodily privacy, locational privacy, or solitude⁴, the US-American concept of informational privacy is quite closely related to the European concept of data protection law. While informational privacy and data protection law are often treated as identical concepts in the media and in public and private debate, it is well understood today that the two concepts need to be distinguished⁵.

- 3 This paper focuses on the idea of informational self-determination and questions this concept's ability to serve as a rationale for European data protection law. It thereby focusses on the all-encompassing regulation of the processing of personal data by private actors as provided for by the GDPR⁶. To this

* Prof. Dr., Professor of Information and Communications Law, Chair of the Executive Board of the Center for Information Technology, Society, and Law (ITSL) and Director of the Digital Society Initiative (DSI) of the University of Zurich. I thank Dr. Stephanie Volz, managing director of the ITSL, for research assistance.

- 1 While there is quite some debate in Germany, there seems to be an almost complete lack of discussion, especially in the UK, and to a lesser extent also in France. Note that most German authors focus on the public sector when discussing the theoretical foundation of data protection law; see: Alexander Rossnagel, 'Kein "Verbotssprinzip" und kein "Verbot mit Erlaubnisvorbehalt", Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff', NJW 2019, 1–5; Wolfgang Hoffmann-Riem, 'Informationelle Selbstbestimmung in der Informationsgesellschaft' in Wolfgang Hoffmann-Riem (ed), *Offene Rechtswissenschaft* (Mohr Siebeck 2010); Gabriel Britz, 'Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts' in Wolfgang Hoffmann-Riem (ed), *Offene Rechtswissenschaft* (Mohr Siebeck 2010) 561–596; Marion Albers, 'Umgang mit personenbezogenen Informationen und Daten' in Wolfgang Hoffmann-Riem and others (eds), *Grundlagen des Verwaltungsrechts* (2nd edn, C.H. Beck 2012) 107–234; Johannes Masing, 'Herausforderungen des Datenschutzes' [2012] NJW 2305–2311; Karl-Heinz Ladeur 'Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?' (2009) 2 DöV 45–55.
- 2 Art. 8 Charter of Fundamental Rights of the European Union.

3 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 193 Harvard Law Review 22.

4 For the different concepts of privacy see: Daniel J Solove, 'Understanding Privacy' (2008) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888> accessed 15 November 2021, 13ff; Helen Nissenbaum, *Privacy in Context - Technology, Policy, and the Integrity of Social Life* (Stanford Law Books 2010) 67ff; Alan F Westin, *Privacy and Freedom* (Atheneum 1967) 77; Charles Fried, 'Privacy' [1968] The Yale Law Journal 475; Ruth Gavinson, 'Privacy and the Limits of Law' (1980) 89 The Yale Law Journal 421; Randall P Bezanson, 'The Right to Privacy Revisited: Privacy, News and Social Change 1890-1990' (1992) 80 California Law Review 1133; Adam Moore, 'Defining Privacy' (2008) 39 Journal of Social Philosophy 411; Bert-Jaap Koops and others, 'A Typology of Privacy' (2017) 38 (2) University of Pennsylvania Journal of International Law 483.

5 Gernot Sydow, 'Artikel 1 DSGVO' in Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung* (2nd edn, Nomos 2018) para 10ff; Orla Lynskey 'Deconstructing data protection: The 'added value' of a right to data protection in the EU legal order' (2014) 63 International and Comparative Law Quarterly 567ff.; Raphaël Gellert and Serge Gutwirth, 'The legal construction of privacy and data protection' (2013) 29 Computer Law & Security Review 522, 523ff.

6 For a critical evaluation of the right to informational self-determination as a fundamental right and a governing principle for the processing of data by government agencies see: Ladeur (n 1) 45; Albers (n 1) 107; Marion Albers, 'Realizing the Complexity of Data Protection' in Serge Gutwirth and others (eds), *Reloading Data Protection* (Springer 2014) 213–235; Britz (n 1) 561–596; Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the

end, the paper first outlines the idea and concept of informational self-determination (B.); second, analyses the fractional implementation of this concept in the GDPR (C.); and third, demonstrates that informational self-determination cannot be considered a feasible rationale for data protection law (D.). The paper concludes with a call for the development of alternatives, both with regard to the need for a convincing rationale and alternative regulatory approaches that can build upon and properly implement such rationale (E.).

B. Idea and Concept

4 The idea and concept of informational self-determination refers to every individual’s right and opportunity to determine which information about him- or herself is disclosed to others and for what purposes such information may be used⁷. In Europe, the notion of an individual’s right to informational self-determination was first articulated by the Federal Constitutional Court of Germany in its landmark decision on the Federal Census Act of 1983⁸.

Herein the Court suspended the carrying out of a population census and ruled that the Federal Census Act must be amended before census may resume. The Court based its ruling on the argument that the rights to human dignity and integrity as enshrined in the Basic Law of Germany provides for a more specific fundamental right of every individual to decide on the disclosure and use of his or her personal information⁹.

5 Since 1983, the term and idea of informational self-determination have had a successful career in legal thinking and in public debate, at least in Europe where the right to informational self-determination has become one of the conceptual foundations for the right to the protection of personal data as enshrined in Art. 8 of the Charter of Fundamental Rights of the European Union¹⁰. Following the decision of the German Constitutional Court in 1983, many even argue that the right to informational self-determination is a fundamental right in itself¹¹. This

Power’ in Erik Claes and others (eds) *Privacy and the Criminal Law* (Intersentia 2006) 61-104; Gellert and Gutwirth (n 5) 522-530; Gloria Gonzáles Fuster *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014); Gloria Gonzáles Fuster and Serge Gutwirth, ‘Opening up personal data protection: A conceptual controversy’ (2013) 29 *Computer Law & Security Review* 531-539; Nikolaus Marsch, *Das europäische Datenschutzgrundrecht* (Mohr Siebeck 2018) 98ff.; Nikolaus Marsch, ‘Artificial Intelligence and the Fundamental Right to Data Protection’ in Thomas Wischmeyer and Timo Rademacher (eds) *Regulating Artificial Intelligence* (Springer 2020) 33-52; Ralf Poscher, ‘The Right to Data Protection: A No-Right Thesis’ in Russel A. Miller (ed) *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge University Press 2017) 129-142; Ralf Poscher, ‘Artificial Intelligence and the Right to Data Protection’ (2021) Max Plank Institute for the Study of Crime, Security and Law Working Paper No. 2021/03 <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3806531_code386115.pdf?abstractid=3769159&mirid=1> accessed 15 November 2021.

7 Schwartz, ‘Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology’ [2011] *William and Mary Law Review* 351, 368; Kenneth A Bamberger and Deirdre K Mulligan, ‘Privacy in Europe: Initial Data on Governance Choices and Corporate Practices’ [2013] *The George Washington Law Review* 1529, 1539.

8 Decision of the Federal Constitutional Court of Germany of 15 December 1983, Az 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 vR 269/83, 1 BvR 440/83,

BVerfGE 65, 1 – Volkszählung.

9 BVerfGE 65 (n 8) 43 - Volkszählung.

10 Peter Gola, ‘Einleitung’ in Peter Gola (ed), *Datenschutz-Grundverordnung: DS-GVO* (2nd edn, C.H. Beck 2018) para 6; Bernd Schmid, ‘Art. 1 DSGVO’ in Jürgen Taeger and Detlev Gabel (eds), *DSGVO BDSG* (3rd edn, Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft 2019) para 25; Jürgen Kühling and Johannes Raab, ‘Einführung’ in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG Kommentar* (3rd edn, C.H. Beck 2020) para 26, see also Antoinette Rouvroy and Yves Pouillet ‘The Right to Informational Self-Determination and the Value of Self-Development’ in Serge Gutwirth and others (eds), *Reinventing Data Protection* (Springer 2009) 51, 68.

11 Schwartz (n 7) 364, 367ff; Brendan Van Alsenoy and Eleni Kosta and Jos Dumortier, ‘Privacy notices versus informational self-determination: Minding the gap’ [2014] *International Review of Law, Computers & Technology* 185, 188; Markus Thiel, *Die „Entgrenzung“ der Gefahrenabwehr* (Mohr Siebeck 2011) 221; Claudio Franzius, ‘Das Recht auf informationelle Selbstbestimmung’ [2015] *Zeitschrift für das juristische Studium* 259; René Rhinow and Markus Schefer and Peter Übersax (eds), *Schweizerisches Verfassungsrecht* (3rd edn, Helbing & Lichtenhahn 2016) para 1376ff; Eva Maria Belser, ‘Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?’ in Astrid Epiney and others (eds), *Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung/Instrumente de mise en oeuvre du droit à l’autodétermination informationnelle* (Schulthess 2013) 25; critical of the characterisation as a fundamental right: Hans Peter Bull, *Informationelle Selbstbestimmung – Vision oder Illusion?* (2nd edn, Mohr Siebeck 2011) 45ff; Alexandre Flückiger, ‘L’autodétermi-

approach has also been adopted by the Swiss Federal Supreme Court¹² even though the Swiss Federal Constitution solely provides for a right of every person to be protected against the misuse of his or her personal data (Art. 13 (2) Swiss Federal Constitution). The right to informational self-determination has also evolved regarding its content. For some authors, this right does not only allow individuals to decide on the disclosure and use of information about them but grants them full control of the use of “their” personal data¹³.

- 6 In contrast, the German Federal Constitutional Court has significantly attenuated its understanding of the right to informational self-determination in a relatively recent decision by stating that this right does not confer a general or even comprehensive right to self-determination with regard to the use of one’s own personal data; instead, it shall only provide individuals a right to have a substantial say in the making available and the use of their personal data¹⁴.
- 7 Regardless of this remarkable confinement, the aforementioned view according to which the right to informational self-determination grants every individual a right to decide on the disclosure and use of his or her personal information is still the predominant understanding of the idea and concept of informational self-determination in Europe. Most prominently, this “classical” understanding of informational self-determination has been adopted by the French legislator who explicitly states in its law on electronic data processing, files and freedoms that every individual has a right to decide on and control the use of their personal data and that this right must be exercised within the framework of the GDPR and the aforementioned national law¹⁵.

nation en matière de données personnelles: un droit (plus si) fondamental à l’ère digitale ou un nouveau droit de propriété?’ [2013] Aktuelle Juristische Praxis, 837 passim; Thomas Gächter and Philipp Egli, ‘Informationsaustausch im Umfeld der Sozialhilfe – Rechtsgutachten’ (Jusletter, 6 September 2010) <https://jusletter.weblaw.ch/jusissues/2010/583/_8587.html> accessed 15 November 2021, para 21ff.

- 12 Swiss Federal Supreme Court (BGE 146 I 11) [2019] at 3; Swiss Federal Supreme Court (BGE 145 IV 42) [2018] at 4.2; Swiss Federal Supreme Court (BGE 143 I 253) [2017] at 4.8; Swiss Federal Supreme Court (BGE 142 II 340) [2016] at 4.2; Swiss Federal Supreme Court (BGE 140 I 2) [2014] at 9, all with further references.
- 13 Rouvroy and Pouillet (n 10) 45.
- 14 BVerfGE – 1 BvR 16/13, 87.
- 15 Art. 1 al. 2 de la loi n. 78-17 du 6 janvier 1978 relative à

- 8 Even if one agrees that the right to informational self-determination is a fundamental right, this right may only serve as a rationale for regulating the processing of personal data by government agencies. Such regulation(s) would have to define what personal data government agencies may collect about their citizens and under what conditions and for which purposes the data may be processed. But as private actors are not (directly) bound by fundamental rights¹⁶, informational self-determination cannot readily serve as a rationale for regulating the processing of personal data by private actors¹⁷. Instead, a more in-depth analysis is needed.

C. Actual Implementation

- 9 The GDPR hardly provides any guidance as to its rationale. The wording of its objective is very broad and general. According to Art. 1 (2) GDPR the regulation aims at protecting “fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data”. Even though this objective may serve as a (quite unspecific) guidance for the processing of personal

l’informatique, aux fichiers et aux libertés: «Les droits des personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel les concernant et les obligations incombant aux personnes qui traitent ces données s’exercent dans le cadre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 et de la présente loi.

- 16 Art. 51 Charter of Fundamental Rights of the European Union; Art. 16 para 2 Treaty of the Functioning of the European Union; Art. 1 para 3 Basic Law of the Federal Republic of Germany; Art. 35 para 3 Swiss Federal Constitution *e contrario*; see also Stefanie-Daniela Waldmeier, *Informationelle Selbstbestimmung – ein Grundrecht im Wandel* (Dissertation, 2015), 104 <<https://www.zora.uzh.ch/id/eprint/122636/>> accessed 15 November 2021 and Masing (n 1) 2305.
- 17 This is disregarded by the Federal Constitutional Court of Germany and the Swiss Federal Supreme Court. In BVerfG, 1 BvR 16/13, 85, the German Constitutional Court has stated that there is no reason for not applying the fundamental right to informational self-determination in the relation between private actors. The Swiss Federal Supreme Court has repeatedly stated that the fundamental right to informational self-determination implies that every individual has a right to decide about the processing of personal data about them by government agencies and private actors; see Swiss Federal Supreme Court (BGE 146 I 11) [2019] at 3; Swiss Federal Supreme Court (BGE 144 II 91) [2017] at 4.4; Swiss Federal Supreme Court (BGE 140 I 2) [2014] at 9, all with further references.

data by government agencies, it can hardly serve as a rationale for the all-encompassing regulation of the processing of personal data by private actors given that they are not directly bound by fundamental rights.

- 10 While the provision on the objective of the GDPR does not give clear guidance as to the regulation's rationale, recital 7 provides some by stating that "Natural persons should have control of their own personal data". Although the GDPR does not mention informational self-determination, the idea of natural persons controlling their own personal data is to be considered an identical concept labelled less eloquently. Accordingly, at least in the German speaking part of Europe, many scholars agree that the idea of informational self-determination is the underlying rationale of the GDPR¹⁸.
- 11 The search for a convincing rationale is not merely a theoretical problem since the often very broad notions of the GDPR require an interpretation of the legal text which must be carried out (amongst others) with regard to the purpose of the law¹⁹. By applying these notions in one way or another, scholars, practitioners and – most importantly – supervisory authorities and courts, make implicit assumptions about the rationale of data protection law. Given their impact on the interpretation and application of the GDPR, these assumptions should be made explicit to allow for a critical assessment of the assumed rationale and the resulting decisions.
- 12 If the GDPR aims to put the idea of control or informational self-determination into action, this raises the question if this concept is duly implemented and able to provide a sound theoretical basis for the most important rules and procedures established in the GDPR. The key provisions that must be analysed for this assessment are the principles relating to the processing of personal data (Art. 5 GDPR), the rules on the lawfulness of processing, including the specific provisions on consent (Art. 6 et seqq. GDPR), the rights of the data subjects (Art. 12 et seqq. GDPR), and the rules on the enforcement of the provisions, namely the ones on the competence, tasks and powers of the supervisory authorities (Art. 55 et seqq. GDPR) and the ones on remedies, liability and penalties (Art. 77 et seqq. GDPR).

- 13 The *principles relating to the processing of personal data* (Art. 5 GDPR) can only be explained to a very limited extent by the idea of informational self-determination. Transparency (Art. 5 (1) (a) GDPR), purpose limitation (Art. 5 (1) (b) GDPR) and security of data processing (Art. 5 (1) (f) GDPR) are key prerequisites for informational self-determination as exercising control requires that data subjects are informed about the processing of personal data about them, that this data is not processed for purposes which are incompatible with the ones the data subjects have been informed about, and appropriate security measures are implemented to prevent unauthorised processing and accidental loss or destruction of the data. But the other principles, namely the principles of lawfulness and fairness (Art. 5 (1) (a) GDPR), data minimisation (Art. 5 (1) (c) GDPR), accuracy (Art. 5 (1) (d) GDPR) and storage limitation (Art. 5 (1) (e) GDPR) do not aim at establishing control of data subjects. While these principles may serve legitimate goals, they cannot be based on the concept of informational self-determination.

- 14 Together with the principles of data protection, the rules on the *lawfulness of processing* (Art. 6 GDPR) form the normative core of the GDPR. The most prominently regulated and most intensively discussed reason for the lawfulness of processing of personal data is the data subject's consent (Art. 6 (1) (a); Art. 7 et seq. GDPR). The requirement of consent is evidently a straightforward implementation of informational self-determination. Though many data subjects believe that the processing of personal data about them is usually based on their consent, consent is far from being the prevailing basis for the lawfulness of processing. Unfortunately, there is no empirical evidence available on the relative importance of the various legal grounds for the processing of personal data. But for all practitioners – data protection officers, data protection lawyers and supervisory authorities – it is clear that in the vast majority of cases the lawfulness of processing is not based on consent but on the legitimate interests pursued by the controller (Art. 6 (1) (f) GDPR). In informal exchanges, prominent data protection commissioners have assumed that this is true for more than 90% of data processing activities. Regardless of how accurate this number may be, the relative importance of data subjects' consent and the legitimate interests of controllers as a legal basis for the processing of personal data is very clear. Evidently, the most important legal ground for the processing of personal data is not based on the idea of informational self-determination but on the need of controllers to process personal data in a wide range of situations. The fact that the data subjects' interests are considered when assessing the legitimate interests of the controller does not make any difference as the data subjects have no means to influence the balancing of interests, e.g. by

18 Kühling and Raab (n 10) para 26; Masing (n 1) 2305; Jan Philip Albrecht 'Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung!' [2013] Zeitschrift für Datenschutz 587; critical Winfried Veil, 'Die Datenschutz-Grundverordnung: des Kaisers neue Kleider' [2018] Neue Zeitschrift für Verwaltungsrecht 686, 691.

19 Schmid (n 10) para 19; Pötters, 'Art. 1' in Gola (n 10) para 20.

providing their own point of view on the processing subject to the assessment. The concept of informational self-determination cannot serve as a basis for the other reasons for the lawfulness of processing either, namely the processing for the performance of a contract (Art. 6 (1) (b) GDPR), for compliance with a legal obligation of the controller (Art. 6 (1) (c) GDPR), and for the performance of a task carried out in the public interest (Art. 6 (1) (e) GDPR). The only exception is the processing of personal data for protecting the vital interests of the data subject (Art. 6 (1) (d) GDPR), which is based on the assumption of the data subject's consent²⁰. Given the very limited importance of consent for the lawfulness of processing, it proves impossible to ground the assessment of the legal basis for the processing of personal data on the concept of informational self-determination.

- 15 As opposed to the lawfulness of processing, the *rights of data subjects* (Art. 12 et seqq. GDPR) can clearly be based on the concept of informational self-determination. This holds true for the obligation of controllers to provide data subjects with a wide range of information (Art. 13 et seq. GDPR) and for the specific rights of data subjects, namely the right of access (Art. 15 GDPR), the right to rectification (Art. 16 GDPR), the right to erasure (Art. 17 GDPR), the right to restriction of processing (Art. 18 GDPR), and the right to object (Art. 20 GDPR). But even here, the control of data subjects is limited as some rights come with important restrictions. Namely, the right to erasure is merely granted if one out of a limited set of situations is given, e.g. if personal data is no longer necessary in relation to the purpose for which it was collected (Art. 17 (1) (a) GDPR) or if the data subject withdraws consent and there is no other legal ground for the lawfulness of processing (Art. 17 (1) (b) GDPR). The same is true for the right to restriction of processing even though the situations in which such a right takes effect are different (Art. 18 GDPR). Most importantly, data subjects have no general right to object to the processing of their personal data. Instead, this right is only granted if the processing of personal data is based on the legitimate interest of the data controller (Art. 6 (f) GDPR) or if it is necessary for the performance of a task carried out in the public interest (Art. 6 (e) GDPR). In addition, the right to object must always be exercised on grounds relating to the particular situation of the data subject (Art. 21 (1) first sentence GDPR), e.g. for reasons relating to their family life or for the protection of trade secrets. Even if such reasons are given, the right to object is subject to

another very general restriction since the controller may continue to process the data if it is able to demonstrate compelling legitimate grounds for the processing of the data which override the interests, rights and freedoms of the data subject (Art. 21 (1) second sentence GDPR). Even though compelling grounds may be given in many instances as they have to be assessed in a pondering of interests of the controller on the one hand and the data subject on the other²¹, personal data can be processed in many cases against the data subject's express objection.

- 16 The *enforcement* of data protection law is primarily ensured by supervisory authorities; they are responsible for monitoring and enforcing the application of the GDPR (Art. 57 (1) (a) GDPR). They are vested with far-reaching powers including (amongst many others) the power to carry out investigations in the form of data protection audits (Art. 58 (1) (b) GDPR), to order the controller or processor to bring processing operations into compliance with the provisions of the GDPR (Art. 58 (2) (d) GDPR), to impose a temporary or definitive limitation or a ban on the processing of personal data (Art. 58 (2) (f) GDPR), and, to impose an administrative fine (Art. 58 (2) (i) GDPR). While Supervisory authorities may act in response to complaints of data subjects (Art. 57 (1) (f) GDPR) or initiate investigations themselves as they see fit (Art. 57 (1) (h) GDPR). Although the GDPR grants every data subject a right to an effective judicial remedy against a controller or processor (Art. 79 GDPR) and the right to receive compensation for a damage suffered (Art. 82 GDPR), these rights are hardly used. Instead, the enforcement of the provisions of the GDPR almost entirely banks on the supervisory authorities. While these authorities are certainly convinced to act in the best interest and on behalf of data subjects, the concept of enforcement by an independent supervisory authority can hardly be reconciled with the idea of informational self-determination, i.e. the idea that data subjects decide by themselves about the processing of their personal data.
- 17 The brief analysis of the most important rules and procedures established in the GDPR has revealed that only a limited number of its key provisions can be based on the idea of control or informational self-determination. Most importantly, in about nine out of ten cases the processing of personal data by

20 See also Jürgen Taeger 'Art. 6 DSGVO' in Taeger and Gabel (n 10) para 46; Philipp Reimer, 'Art. 6 DSGVO' in Sydow (n 5) para 3; Benedikt Buchner and Thomas Petri, 'Art. 6 DSGVO', in Kühling and Buchner (n 10) para 109f; Peter Schantz, 'Art. 6 DSGVO' in Simitis and others (eds), *Datenschutzrecht: DSGVO mit BDSG* (Nomos 2019) para 61.

21 Sebastian Schulz, 'Art. 21 DSGVO' in Gola (n 10) para 12; Mario Martini 'Art. 21DSGVO' in Boris Paal and Daniel Pauly (eds), *DS-GVO BDSG* (3rd edn, C.H. Beck 2021) para 29; Tobias Herbst, 'Art. 21 DSGVO' in Kühling and Buchner (n 10) para 19ff; Johannes Caspar, 'Art. 21 DSGVO' in Simitis and others (n 20) para 19; Martin Braun and Hans-Georg Kamann 'Art. 21 DSGVO' in Eugen Ehmann and Martin Selmayr (eds), *DS-GVO: Kommentar* (2nd edn, C.H. Beck 2018) para 22ff.

private actors is based on the legitimate interests of the controller and not on data subjects' consent. Given the key importance of the legal basis for the processing of personal data under the GDPR, the finding alone that most processing of personal data is based on the legitimate interests of the controller and not on data subjects' consent clearly demonstrates that the GPPR does not implement the idea of informational self-determination. This finding is amplified by the fact that the restrictions to the right to object even allow for the processing of personal data against the explicit will of data subjects. The lack of implementation of informational self-determination in the GDPR endorses the finding that this idea and concept cannot be perceived as the underlying rationale for European data protection law.

D. Normative Analysis

- 18 The finding that informational self-determination is not truly implemented in the GDPR despite the intention of the European legislator to grant individuals control of “their” personal data raises serious doubts as to the feasibility of this concept. But this factual finding does not preclude that informational self-determination should be the rationale of data protection law and that the GDPR should be revised to ensure its proper implementation. However, there are also important doubts on a normative level as to whether informational self-determination is a feasible rationale.
- 19 At first, the idea of informational self-determination sounds very convincing. After all, liberty, dignity, autonomy or personal freedom, i.e. the right of every individual to decide about their own life within the limits of the law, are core values shared by most western societies and fundamental rights guaranteed implicitly or explicitly by most constitutions in Europe²². In the relationship between private actors, these core values are reflected in the principle of private autonomy. From this perspective, informational self-determination appears to be a logical, almost inevitable consequence or even part of the general right to self-determination²³. Accordingly, scholars and courts referring to the idea of informational self-determination hardly ever provide an ex-

planation as to why such a right should exist²⁴. This is especially true for recital 7 of the GDPR which fails to provide any explanation as to why natural persons should have control of personal data about them. Given the importance and impact of the idea and concept of informational self-determination, this is astonishing. It seems that lawmakers, courts, and most scholars have been carried away by the persuasive power of an eloquent terminology. Surely, a closer analysis is needed.

- 20 This analysis must distinguish between the relation between individuals and the state and the relation between individuals and other private actors, namely businesses. The relation between individuals and the state is primarily determined by a set of fundamental rights and a set of laws that define and delimit the activities of government agencies. Acknowledging a fundamental right to informational self-determination thus only means that the state may not require citizens to provide information about themselves and government agencies may not use that information without a sound legal basis²⁵. The situation presents differently, however,

24 For Germany: Dietrich Murswiek and Stephan Rixen ‘Art. 2 GG’ in Michael Sachs (ed), *Grundgesetz* (9th edn, C.H. Beck 2021) para 72ff.; Udo Di Fabio ‘Art. 2 Abs. 1 GG’ in Theodor Maunz and Günter Dürig (eds), *Grundgesetz-Kommentar* (94th edn, C.H. Beck 2021) para 174f.. For Switzerland: Swiss Federal Supreme Court (BGE 120 II 118) [1994] at 3a; Swiss Federal Supreme Court (BGE 122 I 153) [1996] at 6b; Swiss Federal Supreme Court (BGE 138 II 346) [2012] at 8.2; Rainer Schweizer, ‘Art. 13 Abs. 2 BV’ in Stephan Breitenmoser and Rainer Schweizer (eds), *Die Schweizerische Bundesverfassung* (3rd edn, Dike 2014) para 72; Regina Kiener and Walter Kälin and Judith Wyttenbach, *Grundrechte – Stämpfli juristische Lehrbücher* (3rd edn, Stämpfli 2018) 178; Jörg Paul Müller and Markus Schefer (eds), *Grundrechte in der Schweiz* (4th edn, Stämpfli 2008) 164f; Waldmeier (n 16) 105.

25 For Germany: Murswiek and Rixen (n 24) para 13ff, 73; Di Fabio (n 24) para 178. For Switzerland: Schweizer (n 24) para 79; Giovanni Biaggini, ‘Art. 13 BV’ in Giovanni Biaggini (ed), *Bundesverfassung der Schweizerischen Eidgenossenschaft: Kommentar* (Orell Füssli 2017) para 11. Art. 52 of the Charter of Fundamental Rights of the European Union states that “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”. With regard to data protection law see Benedikt Buchner ‘Art. 1 DSGVO’ in Kühling and Buchner (n 10) para 16; Heinrich Amadeus Wolff, ‘AEUV Art. 16’ in Matthias Pechstein and Carsten Nowak and Ulrich Häde (eds), *Frankfurter Kommentar EUV/GRC/AEUV* (Mohr Sie-

22 For example: Art. 5 para 1 sentence 1 European Convention on Human Rights; Art. 1 and Art. 6 Charter of Fundamental Rights of the European Union; Art. 1 para 1 and Art. 2 para 2 Basic Law of the Federal Republic of Germany; Art. 7 and Art. 10 Swiss Federal Constitution.

23 In this sense also BVerfGE 65 (n 8) 42ff.

for private actors. According to the principle of private autonomy, private actors are free to pursue all activities they see fit²⁶ and the introduction of limitations calls for justification²⁷. This also applies to the collection and use of personal data. This fundamental problem is mostly disregarded when promoting the idea of informational self-determination. Yet it is obvious that granting individuals a right to control the use of personal data about them inevitably leads to a limitation of all private actors to collect and use such data. Interestingly, such a limitation can hardly be integrated into the broad types of rights the law has developed to govern the relationship between private actors. Private law knows three basic types of rights that allow private actors to restrict the freedom of other private actors: property rights, tort law, and contracts. Of course, this categorisation is a gross simplification, and a much more detailed analysis would be needed to make the necessary distinctions. But looking at these very broad categories nevertheless reveals that a right of private actors to control the processing of personal data by other private actors is hard to integrate into our legal system. In any case, and contrary to what the

notion of informational self-determination implies, a right to informational self-determination does not exist per se in the relationship between private actors and such right cannot be justified by simply stating that the fundamental right to informational self-determination should apply mutatis mutandis to the relation between private actors²⁸. Instead, calling for a right to informational self-determination in the relationship between private actors requires a convincing justification. When looking for such a justification, three aspects should be considered.

- 21 First, all human interaction is based on the processing of personal data. We are constantly processing important amounts of data about others in our brains. But no one would consider that we should have a right to determine what others think about us²⁹. This also applies to business relations, e.g. to a consumer shopping at a local grocery store. The shopkeeper will gather quite some information about the habits, preferences, moods, and financial resources of its customers and no one would call for the introduction of a right that would allow the consumer to control the processing of that data in the shopkeeper's brain. Why should this be fundamentally different if the data was stored on paper or an electronic device? In fact, it is not, as demonstrated by the key importance of the legitimate interests of controllers as a legal basis for the processing of personal data³⁰. It is precisely because all human interaction is based on the processing of personal data that legislators and supervisory authorities cannot help but recognize scores of various instances in which personal data can be processed without data subjects' consent, thereby depriving them of their alleged right to informational self-determination.

beck 2017) para 11, 12; Philip Kunig and Jörn Axel Kämmerer 'Art. 2 GG' in Ingo von Münch and Philip Kunig (eds), *Grundgesetz Kommentar: GG* (7th edn, C.H. Beck 2021) para 78.

- 26 In Switzerland, private autonomy is the basis for economic freedom according to Art. 27 Swiss Federal Constitution; Kurt Vallender 'Art. 27 BV' in Bernhard Ehrenzeller and others (eds), *Die Schweizerische Bundesverfassung: St. Galler Kommentar* (4th edn, Dike 2014) para 51; Bernhard Waldmann, 'Art. 35 BV' in Bernhard Waldmann and Eva Maria Belser and Astrid Epiney (eds), *Basler Kommentar Bundesverfassung* (Helbing Lichtenhan 2015) para 71. In Germany, the concept of private autonomy is covered by Art. 2 para 1 Basic Law of the Federal Republic of Germany, see Udo Di Fabio 'Art. 2 Abs. 1 GG' in Maunz and Dürig (n 24) para 101; Christian Starck 'Art. 2 GG' in Hermann von Mangoldt and Friedrich Klein and Christian Starck (eds), *Grundgesetz* (7th edn, C.H. Beck 2018) para 145; Horst Dreier, 'Art. 2 Abs. 1 GG' in Horst Dreier (ed), *Grundgesetz-Kommentar* (3rd edn, Mohr Siebeck 2013) para 35, 62; Hans Jarass, 'Art. 2 GG' in Hans Jarass and Bodo Pieroth (eds), *Grundgesetz für die Bundesrepublik Deutschland - Kommentar* (16th ed, C.H. Beck 2020) para 22; Kunig and Kämmerer (n 25) para 78.
- 27 According to art 36 para 2 Swiss Federal Constitution restrictions on fundamental rights such as economic freedom must be justified by a public interest or by the protection of the fundamental rights of third parties; see also Biaggini (n 25) para 29; Vallender (n 26) para 57. The same applies in German law, see Di Fabio (n 24) para 104; Starck (n 26) para 19ff; Horst Dreier, 'Art. 2 Abs. 2 GG' in Dreier (n 26) para 47.

28 In this sense, for Germany: Masing (n 1) 2307f. For Switzerland: Swiss Federal Supreme Court (BGE 146 I 11) [2019] at 3.1.1; Swiss Federal Supreme Court (BGE 144 II 91) [2017] at 4.4; Swiss Federal Supreme Court (BGE 142 II 340) [2016] at 4.2, all with further references. In a similar way, but without referring to the idea of informational self-determination: De Hert and Gutwirth (n 6), stating that similar rationales apply with regard to the regulation of the processing of personal data in the public and the private sector.

29 Likewise: Masing (n 1) 2307. This problem has already been addressed in the seminal decision of the Federal Constitutional Court of Germany. The court has rightly pointed out that personal information is a reflection of social reality that cannot be exclusively assigned to a specific individual, which is why all individuals must accept restrictions on their right to informational self-determination; BVerfGE 65 (n 8) 1, 44 - Volkszählung.

30 See above, C.

22 Second, the concept of informational self-determination only makes sense if individuals care about the collection and usage of personal data about them. In other words, granting individuals control over the use of personal data is only meaningful if they actually exercise this control. Yet this is hardly the case. Only few data subjects use the rights granted by the GDPR and many studies show that privacy policies are hardly read³¹. Instead of exercising our supposedly important right to informational self-determination, most of us just click *accept* whenever we are asked if we agree to the processing of data about us. The lack of exercise also raises the question of whether the (limited) amount of control which is granted today is of any benefit to individuals. Even if one assumes that the mere possibility to exercise (some) control has a certain value for data subjects, the benefits created must be weighed against the costs incurred for granting that control. While reliable numbers are not available, one may infer from anecdotal evidence that the costs for establishing compliance with the GDPR are in the three-digit million range for the big tech companies and in the two-digit million range for many other large companies that serve customers in the EU³². And this solely in-

cludes the direct costs for compliance while disregarding the much greater costs of lost opportunities. Namely the costs for research and development and innovative business models which are not possible at all or are not carried out because of the limitations for the use of personal data and the liability risks caused by the GDPR. From this perspective, it can hardly be assumed that a regulation which is built on the concept of informational self-determination will create greater benefits than costs for society at large.

23 Third, data is a public good³³. Such goods are characterised by two features: they can be used simultaneously by an unlimited number of persons without the use by one person affecting the use by another (non-rivalrous use) and no one can exclude others from the use of these goods (non-excludable use). Given the non-rivalrous use, the benefit of a public good for society is greatest, if it can be used by everyone. Accordingly, legal instruments that allow an individual to restrict the use of such goods should be granted only if such restrictions are needed to achieve other important policy goals. With regard to private actors, two aspects are key. First, a legal intervention is necessary if needed to protect individuals from harms caused by others; second, an intervention is needed in case of market failure, e.g. if a good valuable to society would not be produced if the producer were unable to reap the benefits it created³⁴. The latter need for intervention has been debated in connection with the demand for the cre-

31 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policy Makers, FTC Report, March 2012 2, 61; Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880, 1884ff; Aleecia M McDonald and Lorrie F Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543, 565, estimate that it would take 201 hours annually for an American Internet user to read the privacy policies of all the services they use.

32 Concrete and reliable figures are not yet available and most companies will be reluctant to publish them. However, some indications can be gained from few publicly available statements. For example, according to an estimate by Forbes, compliance with the requirements of the GDPR costs Fortune 500 companies around \$16 million; see Oliver Smith, 'The GDPR Racket: Who's Making Money From This \$9bn Business Shakedown' (Forbes, 2 May 2018) <<https://www.forbes.com/sites/oliver-smith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#4727a86434a2>> accessed 15 November 2021; similarly, Jeremy Kahn and Stephanie Bodoni and Stefan Nicola, 'It'll Cost Billions for Companies to Comply With Europe's New Data Law' (Bloomberg Businessweek, 22 March 2018) <<https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law>> accessed 15 November 2021; Rita Heimes and Sam Pfeifle, 'Study: GDPR's global reach to require at least 75,000 DPOs worldwide' (iapp, 9 November 2016) <<https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/>> accessed 15 November

2021.

33 For the notion of a public good: Richard A Posner, *Economic Analysis of Law* (9th edn, Aspen Publ 2014) 402; Robert Cooter and Thomas Ulen, *Law and Economics* (6th edn, Berkeley Law Books 2016) 40; Hans-Bernd Schäfer and Claus Ott, *Lehrbuch der ökonomischen Analyse des Zivilrechts* (6th edn, Springer 2020) 86f. With regard to data: Herbert Zech, *Information als Schutzgegenstand* (Mohr Siebeck 2012) 107ff; Thomas Heymann, 'Rechte an Daten, Warum Daten keiner eigentumsrechtlichen Logik folgen' [2016] *Computer und Recht* 650, 652ff; Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' [2016] *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 989, 992ff; Lothar Determann, 'No One Owns Data' (2018) 70 *Hastings Law Review* 1, 41; Florent Thouvenin and Rolf H Weber and Alfred Früh, *Elemente einer Datenpolitik* (Schulthess 2019) 9ff, with further references.

34 Josef Drexler and others, 'Data Ownership and Access to Data' (2016) Max Planck Institute for Innovation and Competition Research Paper No. 16-10, 2ff; Wolfgang Kerber, 'Governance of Data: Exclusive Property vs. Access' (2016) 47(7) *International Review of Intellectual Property and Competition Law* 759, 760; Thouvenin and Weber and Früh (n 33) 36ff.

ation of some kind of “data ownership”³⁵. Today, it is widely accepted, however, that there is no market failure with regard to the production of personal data,³⁶ and that legislators should not grant any property rights in data, neither to businesses for the data they have collected nor to individuals with respect to data about them³⁷.

- 24 If one lets go of the idea that personal data somehow “belongs” to the data subject, there is no convincing reason why an individual should be able to control the use of data about it by a private actor as long as the processing of such data does not cause the individual any harm. While the latter rationale for legal intervention can hardly be doubted and cases of harm such as discrimination or manipulation based on the processing of personal data actually occur, it is also obvious that the need to avoid and remedy harm is unable to support the idea of informational self-determination and to justify the granting of a right that allows individuals to control the processing of personal data about them by other private actors.

E. Conclusion

- 25 The above analysis demonstrated that the idea and concept of informational self-determination cannot serve as a convincing rationale for the all-encompassing regulation of the processing of personal data by private actors. With regard to private actors, informational self-determination is not properly implemented in the GDPR and there are no convincing reasons why this should be the case. As a consequence, the idea and concept of informational self-determination should be abandoned.

- 26 This raises the question as to potential alternatives both regarding the rationale of data protection law and the implementation of such rationale in an alternative regulatory framework. While such alternatives cannot be developed in this paper, it seems possible to identify the most important goals of an alternative approach. First, the law should protect the informational privacy of all individuals and second, it should ensure that no one is harmed by the processing of personal data about them. In addition, some sector-specific rules may be necessary to contain the market power of the big tech companies, namely platform providers. As opposed to hopes and promises voiced when enacting the GDPR, data protection law is not a suitable instrument to achieve this goal.

- 27 The importance of informational privacy and the need to protect it against unwanted interference is hardly contested. While there is some overlap between the idea of informational self-determination and the idea of informational privacy, the latter concept becomes much clearer if the former is abandoned. The protection of informational privacy would ground on every individual’s right to decide what information about them is made available to others, but it would not allow for individuals to control the further use of such information once it has been made available to others. This rationale would allow to abandon some of the most important and most questionable approaches of the GDPR and other data protection laws, namely the need to provide a legal basis for every processing of personal data and the obligation to process such data according to some very general principles such as purpose limitation, data minimisation and storage limitation. Other concepts of data protection law would still be key, namely the principle of transparency, which allows individuals to know what personal data is being collected, and the principle of security, which requires controllers and processors to ensure a sufficient level of data security.

- 28 As with the need to protect informational privacy, the need to ensure that no one is harmed by the processing of personal data about them is widely recognised. The GDPR tries to achieve this goal through its comprehensive regulation which seeks to mitigate the risks that may be caused by the processing of personal data (risk-based approach³⁸).

35 Thouvenin and Weber and Früh (n 33) 36ff, with further references; Michael Dorner, ‘Big Data und «Dateneigentum», Grundfragen des modernen Daten- und Informationshandels [2014] Computer und Recht 617, 625 with further references.

36 Drexl and others (n 34) 2ff; Josef Drexl, ‘Designing Competitive Markets for Industrial Data – Between Propertisation and Access’ (2016) Max Planck Institute for Innovation and Competition Reserach Paper No. 2016/13 30ff; Florian Faust, ‘Ausschliesslichkeitsrecht an Daten?’ in Stiftung Datenschutz (ed), *Dateneigentum und Datenhandel* (Erich Schmidt Verlag 2019) 85, 99; Kerber (n 33) 992ff; Thouvenin and Weber and Früh (n 33) 56ff.

37 Thouvenin and Weber and Früh (n 33) 89ff. For an overview of the scholarly papers and the opinion of the Swiss legislator see Thouvenin and Weber and Früh (n 33) 21ff.

38 Horst Heberlein, ‘Art. 5 DSGVO’ in Ehmann and Selmayr (n 21) para 30; Markus Schröder, ‘Der risikobasierte Ansatz in der DSGVO’ [2019] Zeitschrift für Datenschutz 503; the risk-based approach is also reflected in Art. 35 GDPR on the data protection impact assessment, see Moritz Karg, ‘Art. 35 DSGVO’ in Simitis and others (n 20) para 2; Mario Martini, ‘Art. 35 DSGVO’ in Paal and Pauly (n 21) para 2; Ulrich Baumgartner ‘Art. 35 DSGVO’ in Ehmann and Selmayr (n 21) para 12.

However, by focussing on mitigating largely unknown and unspecific risks, data protection law often fails to protect individuals against the realisation of these risks, i.e. from the actual harms that may be caused by the processing of personal data such as discrimination and manipulation. By providing specific legal remedies, an alternative approach could not only grant individuals appropriate means to remedy such harms but also provide powerful incentives for businesses to avoid the occurrence of such harms in the first place.