Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part II

Controlling Risks Through (not to) Article 8 ECFR Against Other Fundamental Rights

Maximilian von Grafensteina*

There may be no other fundamental right of the European Charter of Fundamental Rights (ECFR) that raises more questions on the precise object and concept of protection than the right to data protection in Article 8 ECFR. A prominent example is the principle of purpose limitation. The preceding first part of this three-parted series has shown how this ambiguity creates various problems both on the conceptual level of fundamental rights as well as on the level of ordinary law (esp. the GDPR). However, it has also been shown how a re-connection of data protection law to concepts of risk regulation may help clarify these ambiguities. On this basis, the second part of this series demonstrates in detail why data protection laws apply a risk-based approach and why this protection strategy is more effective than a harm-based approach. Further, it is possible to assess whether data protection laws apply certain concepts of the precautionary principle and/or the risk-based approach (in the Anglo-Saxon meaning), and if both, which elements of the law may belong to which strategy. The concept proposed in this chapter will promote, focusing on the principle of purpose limitation, a combination of both strategies leading not only to more effective but also more proportionate protection. The last chapter of this second part will demonstrate why all this makes the fundamental right to data protection in Article 8 ECFR indispensable with respect to the other fundamental rights.

Keywords: Article 8 ECFR | fundamental right to data protection | precautionary principle | risk-based approach | GDPR | regulating risks | effects on public and private actors | scope of application | principle of purpose limitation | consent | data protection by design | data protection impact assessment

I. Introduction: Re-connecting Data Protection Law With Concepts of Risk Regulation

The preceding first part of this three-parted series has shown how an ambiguous object and concept of protection of the fundamental right to data protection, as enshrined under Article 8 ECFR, creates various fundamental problems both on the conceptual level of fundamental rights as well as on the level of ordinary law (especially of the GDPR). However, the first part has also shed light on how a re-connection of data protection law to concepts of risk regulation may help clarify the ambiguous object and concept of protection. To this aim, the last chapter of the first part has clarified the concepts behind the terms "harm" and "risk-based approaches" as well as of the

* Maximilian von Grafenstein LL.M. is Professor for ‘Digital Self-Determination’ at the Berlin Career College of the University of the Arts in Berlin (UdK), part of the Einstein Center Digital Future (ECDF) as well as co-head of the research program Governance of Data-Driven Innovation at the Alexander von Humboldt Institute for Internet and Society. For correspondence: <max.von-grafenstein@huig.de>.
"precautionary principle". On this basis, this second part of the series shows, specifically, how such a clearer understanding of different risk regulation concepts can significantly help to refine the object and concept of data protection law. These considerations especially help to explain why data protection law applies a risk-based approach and why this protection strategy is indeed more effective than a harm-based approach. It is furthermore possible to assess whether data protection law applies certain concepts of the precautionary principle and/or the risk-based approach (in the Anglo-Saxon meaning), and if both, which elements of the law may belong to which strategy. The concept proposed in this chapter will promote a combination of both strategies because this leads not only to more effective but also more proportionate protection. The last chapter of this part of the series demonstrates why all this makes the fundamental right to data protection in Article 8 ECFR indispensable with respect to the other fundamental rights.

II. Why a Proactive Risk-based Approach is More Effective than a Reactive Harm-Based Approach

Explaining why a proactive risk-based approach is more effective than a reactive harm-based approach requires to be clear about the difference between regulating the processing of data and the use of information. It should be noted, in this regard, that my contribution does not seek to address in depth the details of the debate about which term ("data" or "information") may serve as a more appropriate legal link for regulation. Instead, this paper seeks only to demonstrate the impact of such a difference on understanding data protection law as a risk regulation and, on this basis, the interpretation of the respective legal instruments. From a risk-regulatory point of view, this will also make clear why the regulator puts the processing purpose into the center of the legal system instead of the processing context, as proposed by Nissenbaum, for instance. Finally, understanding power asymmetries caused by personal data processing as the actual reason for the chosen risk regulation strategy in data protection law helps to set a first threshold for legal data protection.

1. Controlling Data to Protect Against a Potential Abuse of the Retrieved Information

Many scholars define the difference between data and information describing data as signs stored on physical carriers, either in analogue form, e.g. text, audio or video documents, or digitally as on memory chips or hard drives; information, in contrast, is the result of interpreted data – or more precisely, in order to be meaningful, data must be interpreted in relation to a certain context. This includes the situation where information (i.e. the interpretation of data) is buried in data and later extracted again. A meaningful extraction, however, always requires interpreting the signs in relation to a certain usage context. This difference is essential for the assessment of the appropriate protection strategy and measures, i.e. if one sees the information, not the data, as the primary basis for social interaction that may or may not affect an individual. Therefore, an individual is usually more directly affected by the use of the gathered information than by data processing as such. However, although the information is the more direct source that may concern an individual, linking legal protection instruments to data, rather than to information, can be more effective to ensure protection. The reason for this is that it may be more difficult to regulate – using an offhand notion – “what happens in somebody’s head”, i.e. how a person interprets data and what she does on this informational basis, than to regulate the formal source, i.e. the processed data before it becomes in-

1 See a visualisation of this concept at M von Grafenstein and L Wunderlich, The concept of data protection law, in: PinG (1) (2020), freely accessible under <https://zenodo.org/record/3968996>

2 See the brief overview at Nadezhda Partova, ‘The Law of Everything. Broad concept of personal data and future of EU data protection law’ (2018) 10 Law, Information and Technology 1, 50 et seq., who, however, also tries to avoid to go too much into the details.


formation.\(^5\) This difficulty was in fact recognized early on in the debate on data protection and privacy. For example, as early as 1969, the legal scholar Miller stressed that:

“the most effective privacy protection scheme is one that minimizes the amount of potentially dangerous material that is collected and preserved; a regulatory scheme that focuses on the end use of the data by governmental or private systems might be a case of too little, too late.”\(^6\)

The reasoning behind this statement is that the moment data becomes information, it seems – using another offhand notion – to be like “letting a cat out of the bag”. It is difficult to get the cat (information) back. This means regarding the previous considerations that a risk-based approach focusing on data is more effective than a risk-based (or even harm-based) approach focusing on the use of the gathered information. The first reason for this is that when another person retrieves information about an individual gathered from processed personal data, in exactly this moment this person actually gets insight into the individual’s private life what may harm her right to privacy (supposed that this insight exceeds a certain “threshold of relevance” from a normative viewpoint, such as in the light of Article 7 ECFR). This harm is irreparable because it is impossible to delete that information from the person’s memory. The second reason is that it is difficult to prove, once a person has the information, whether this person passes this information on to further persons and whether one of them takes, on the basis of this information, a decision that undermines other rights of the individual, such as to freedom or equality (e.g. by transparent profiling of job applicants).\(^7\) Therefore, it is more effective to regulate the data before a person gets access to and uses the information buried in the data, i.e. as long as only the machine is processing the data or, even earlier, before the data is collected.

Applying these considerations to an individual’s privacy, freedom or equality, which may be threatened or harmed by the use of information, one may come to the following conclusion, for instance: as long as no person gets effectively access to information about an individual (which hence is still buried in data), one may consider this not yet as a harm but as a specific risk to the right to privacy (specific, since it is reasonable to assume that sooner or later the person who is controlling the machine gets access to the data and retrieves the information). In contrast, as long as the information is not used in a way that directly affects the individual, there might just be an unspecified risk to the rights to freedom or equality (unspecific as long as there is no reasonable ground to assume that a person intends to use the information in that way). Of course, these examples shall not give definite answers on which kind of processing poses harm, a specific or an unspecified risk to these rights to privacy, freedom or equality, but they may serve as an inspiration for further discussion in the future.

In conclusion, even if a legislator decides to focus on data as the main legal reference for its regulation, one has to keep in mind that it is the information that, as the more direct source for social interaction, leads to (potentially negative) effects on the individual. This mediatory nature of data and the context-dependency (contextual nature) of information must be taken into account when interpreting data protection law in the search for an appropriate protection. Since information cannot artificially deleted in a person’s memory and it is hard to prove whether information has been passed on to other persons and whether it has been used for potentially negative decisions, it is more effective to apply a risk regulatory approach tying into data (as the basis for information) than to regulate the information itself.

2. The Processing Purpose Refers to the Future Context of an Informational Use

Given the context-dependency of information, one must be aware that the appropriateness of protection

---

5 This observation includes situations where a decision is exclusively made and enforced by a self-learning machine and no human mind (or ‘head’) is directly involved; also in such a situation, the regulator is confronted with the challenge not to know how exactly the machine has made its decision; cf Tal Zarsky, ‘The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making’ (2016) 41 Science, Technology & Human Values 1, 118-132, arguing that transparency will only be one part of an overall effort on the true nature and possible shortcomings of algorithmic governance.


7 See the example at Max van Graafestein, ‘The Principle of Purpose Limitation: The Risk-Based Approach, Legal Principles and Private Standards as Elements for Regulating Innovation’ (Nomos, 2018) 35 et seq.
measures focusing on data (as the raw material for information) also depend on the expected information usage context. This leads to the following question of how to define an informational context. This question was raised in particular by Nissenbaum. In her work on “contextual integrity” she states that an appropriate protection requires indication of how personal data may flow in a particular context. Without going into more detail, what makes Nissenbaum’s thoughts interesting for this contribution is how she tries to define a context and the informational norms that determine the context. Using examples such as education, health care, family, religion, employment or commercial market places, she concludes that “the activity of fleshing out the details of particular types of contexts (...) is more an exercise of discovery than of a definition.” Interestingly, in contrast to this empirical approach, she implies a more normative approach regarding the “informational norms” that determine the context. Nissenbaum refers here to the contextual “values” or, synonymously, “objectives” and “ends”, that play a crucial role in defining whether a certain information sharing practice violates the contextual integrity of the information. It is this reference to “values” what makes her work interesting for this contribution, because the reference to “values” illustrates the need for a normative concept that helps to define the standards that govern how personal information may be used in a particular context. As will be shown in more detail in the next sections, I think (like Albers and Britz, two critics of the German right to informational self-determination) that the variety of the data subject’s fundamental rights serve as an excellent starting point for defining these social contexts or, more precisely, the normatively respected need for protection in these contexts.

However, before that, another aspect should be emphasized. This aspect becomes clear when Nissenbaum promotes the context-based approach as “something materially different, something better” than the purpose-based approach. The reason, in her view, is that the latter would open up a “glaring loophole” as there are no reliable criteria for defining a purpose. However, contrary to her opinion, the purpose-based approach is not anything “materially” different. Rather, a processing purpose does nothing less than indicating in advance the contexts in which a controller wants to collect personal data or will subsequently process the data (or use the gathered information). From this perspective, the purpose-based approach is therefore not materially different, but only procedurally different. The purpose-based approach is merely another legal link that provides protection before the use of information in Nissenbaum’s terminology violates the “contextual integrity” of the information. Thus, the purpose-based approach requires and enables the controller to evaluate appropriate protection measures in a timely manner, i.e. before a possible violation of the contextual integrity of the information occurs. From this perspective, such an extension of protection (over time) pursues the same objective as linking legal protection instruments to data (as the source for information), rather than referring directly to information. Both approaches aim to focus on a point in time when protection is timely enough to provide an effective protection (i.e. a proactive risk-based rather than a reactive harm-based protection).

In conclusion, both mechanisms aim to provide protection before it is too late: linking legal protection to the processing of data, i.e. before data is interpreted and becomes information, is more effective, as it is more difficult (if not impossible) to regulate what people think and do because they got certain information, than to regulate data as the source of information. Similarly, requiring controllers to specify the purpose of their processing enables them to implement appropriate protection measures before the data gets interpreted and used in a specific context, thus causing real harm to an individual. However, even if Nissenbaum misunderstands and, as a consequence from this, underestimates the purpose-based approach, her work makes clear how crucial a normative approach is for assessing the appropriateness of protection.

---

9 See H Nissenbaum, ibid., pp. 127 et seq.
10 Ibid 134
11 Ibid 181.
12 (n 8); (n 4).
3. Power Asymmetry Caused by Data Processing as the Threshold for Legal Protection

Even if data and information is commonly seen as an important part of protection, it is per se not enough to justify protection. Since in the very end, everything consists of information, there was protection without a specific reason. Of course, going back into the origins of the data protection and privacy debates, the problem was never seen in information per se but in informational power asymmetries. The computer scientist Pohle goes into detail on the historical origins of the idea of data protection (as well as privacy and surveillance), in particular of its discussed problems and solutions. He summarizes the beginning of the debate that had recognized the structural advantage of organizations to process information and make (information-based) decisions as an already existing problem of power asymmetry. However, while such a mere “organisational power asymmetry” has already been controlled by the former law, the use of information technologies caused another major shift in the informational power asymmetry. Scholars realized then that they had to re-assess the former protection goals and mechanisms in the light of such organisations that started to undermine the promises of freedom and participation of a modern civil liberty society by means of information technologies. This reason of data protection is therefore an important first step to limit the ever increasing scope of data protection law that supersedes all other fundamental rights, since not all informational power asymmetries are caused by the processing of personal data and can hence be addressed by the applicable other fundamental rights alone.

Against this background it is interesting to see how legal courts conceptualize the problem and solution with respect to data processing. The German Constitutional Court considers, for example that the automated processing of personal data is the issue, since it enables a controller to collect and store the data in a technically unlimited way, and to immediately retrieve the data at any time and anywhere and to combine them into relatively extensive profiles and/or use them for many other purposes. In contrast, the ECtHR, with respect to the human right to private life in Article 8 ECHR, lowers the threshold for the risk perception taking into account that data can be stored permanently and systematically and could harm an individual’s reputation (especially if the data turns out to be wrong). Such a risk perception does not require the automated processing of personal data, but the analogous storage of personal data can already justify legal protection. Against this background it is interesting to see that the right to data protection under Article 8 ECHR sets the threshold for affirming a relevant risk at the moment when a controller processes personal data of an individual. Thus, the question is whether the ECJ sees the reason for data protection – like the German Constitutional Court – in the automated processing, or – like the ECtHR – rather in the systematic and permanent storage of personal data.

In its recent Jehovah’s Witnesses vs. Finland case, the ECJ ruled directly on the grounds of Art. 2 lit. c Data Protection Directive, so that one cannot draw immediate conclusions on the interpretation of Article 8 sect. 1 ECHR. However, it is possible to demonstrate in this case that the informational power asymmetry can work as a useful criterion to assess the need for protection. In this case, the organisation Jehovah’s Witnesses did not automatically process personal data, but only manually stored information on the individuals visited by their door-to-door preachers in a manner that facilitated the retrieval

---

16 ibid 246.
18 Cf the reasoning of the ECtHR, Decision from 25th September 2011, application no. 44787/08 (P.G. and J.H. vs The United Kingdom), cip. 57, referring to ECtHR, Amsan vs Switzerland (GC), no. 27798/95, §§ 63 bis 67, ECHR 2000-II, as well as Rotaru vs Romania (GC), no. 28341/95, §§ 41 bis 44, ECHR 2000-V.
19 See ECJ C-25/17 (Jehovah’s Witnesses), cip. 52 subseq.
20 Differently but also referring to the concept of risk (especially, given the sensitive information concerned), Raphaël Gellert, ‘Door-to-Door Preaching by Jehovah’s Witnesses Community Falls under Data Protection Law’ (2018) 3 EDPL 395.
of this information for future visits. Even if the organisation itself did not come into direct contact with this personal information, but only had the non-personal (geographical) criteria that facilitated the retrieval of this information, the Court confirmed the application of data protection law. Informational power asymmetry created by this kind of filing system can serve as a reasonable explanation that indeed justifies the decision, even if it sets the threshold for protection very low. If one applies this thought to Article 8 ECFR, this would mean that the term “processing of personal data” (in its section 1) does not require the automation of the processing but that any system that facilitates the retrieval of information and, thus, increases the informational power asymmetry justifies protection. However, even if this understanding sets the threshold for protection fairy low, other cases, which have become famous for their absurdity in recent years, can still be excluded from the scope: For instance, the attachment of doorbell signs does not fall, despite some apologists, under the scope of data protection law because their function is not to make information about residents easier to find, but to identify residents as residents on site. Even clearer: The exchange of business cards does not fall within the scope of data protection law because they are exchanged between more or less “equal” communication partners and thus do not create an asymmetry of information power. For the same reason, data protection laws often foresee a so-called household exemption because there is typically no informational power asymmetry between household members, at least, not one that requires protection through a public law.21

Anyway, if one takes the informational power asymmetries caused by the processing of data as the reason for data protection law, one must avoid an overly formnalistic approach either affirming legal protection by applying the protection measures all at once or denying such a protection as a whole. Instead, one must ask at which moment which protective measure is necessary to avoid that the power asymmetry leads to a situation where the processing risk turns into harm, before it is too late. In these cases, preventive or even precautionary protection measures are usually not disproportionate.

III. How Does Data Protection Law Control ‘A Risk to a Right’?

It is clear that the proposed object and concept of protection for Article 8 ECFR must be more specific than just that. To this end, this part aims in particular to clarify the following aspects: First, how exactly should a risk to a more or less specific legal object of protection (let’s say a “risk to a right”) be conceptualized? Secondly, what is the actual function of the purpose limitation principle within this concept, in particular, which role may this principle play in respect to the different risk protection strategies, such as prevention and precaution? And what are typical precautionary and preventive measures to prevent “risks to rights” from turning into a harm?

1. Protecting Autonomy Against Unspecific and Specific Risks (Which are Specified by all Other Fundamental Rights)

Notwithstanding the long tradition of understanding data protection law as regulating risks (or dangers, threats, and so on) of the processing of personal data, the explicit reference to risks in the GDPR triggered a lively debate on how “a risk to a right” should be methodically treated. The legal scholars van Dijk, Gellert and Rommetveit in particular observed an introduction of quantitative risk assessment methods from IT security and environmental law into data protection law. In their opinion, the transfer would “direct risk assessment exercises to the consequences of technologies (ICTs) upon citizens’ fundamental rights” and therefore lead to the question on how such a “risk to a right” should be conceptualized.22 While it is very welcome that the authors are drawing the attention of the current data protection law debate on this issue at all, two things should not be overlooked: First, the idea of data protection (law) as a protection against data processing risks is old, as was shown, leading even back to the

21 See Max van Grafenstein, ‘Kommentar zu Art. 2 der Datenschutz-Grundverordnung’ in Gierschmann, Schlender, Stenzel (Eds.), Kommentar - Datenschutzgrundverordnung (Bundesanzeiger Verlag, forthcoming).
origins of the data protection and privacy debate. And second, in the debate on the regulation of risks independently of the debate on privacy and data protection law, the question has also been raised as to how quantitative measures should be weighed against a qualitative risk to a right. This means that the basic problem has been known before the GDPR came into force – and actually it is not too difficult to solve.

The first step to solve this problem is to clarify what “right”, i.e. which object of protection, is actually at risk. In doing so, this proposal ties in with another traditional strand of the data protection debate, arguing that it is the individual’s autonomy that is at risk from the processing of personal data and that Article 8 ECFR protects. However, since the concept of autonomy is too broad to define precisely all the conditions of data processing (and the use of the retrieved information) in all imaginable contexts, the substance of an individual’s autonomy must (and can also) be further specified by the other fundamental rights. What this means becomes more clear with respect to the refinement of the concept of protection of Article 8 ECFR.

This is the second step to solve the problem of how to conceptualize a “risk to a right”. The concept of protection of Article 8 ECFR does not entail either a precautionary protection against unspecific risks or a preventive protection against specific risks, but both: Providing protection against unspecific risks, Article 8 ECFR opens up its scope of application in a very early stage when personal data is collected, regardless of the exact way in which the personal data are further processed and the retrieved information is used. The fact that personal data is collected is therefore sufficient as a “reasonable ground” for considering that the subsequent processing may lead to a harm for an individual’s autonomy, even if there is not yet sufficient evidence of a causal link between the processing and harm to the autonomy of an individual. As long as there is no such sufficient proof, there is an “unspecific risk” (for the individual’s autonomy). However, the concept of protection of Article 8 ECFR is not limited to this early stage, i.e. an “unspecific risk” against autonomy. Instead, the right to data protection equally guarantees protection if the risk against autonomy gets more specific, i.e. if there is sufficient proof of a causal link between the data processing and harm to an object of protection, which specifies how an individual may exercise her autonomy in a certain context that is covered by another fundamental right. The other fundamental rights can therefore provide an objective and nuanced scale to assess the risks with respect to the context in which the data (more precisely, the gathered information) is used in a specific way. Consequently, the diversity of all data subject’s fundamental rights can help to assess the appropriate protection measures that a controller must implement to prevent such risks that are identified.

Such an object and concept of protection of the right to data protection in Article 8 ECFR leads to the conclusion that the so-called risk-based approach is less concerned with the risk to the fundamental right to data protection than concerned that the right to data protection controls the processing risks to the other fundamental rights. More specifically, the right to data protection reacts to the risk that the processing of personal data may undermine the data subject’s autonomous exercise of her other fundamental rights: Thus, the fundamental right to data protection in Article 8 ECFR controls the risk of personal data processing to the autonomous exercise of all data subjects’ other fundamental rights.

On this basis, the methodology of the data protection risk assessment can be further clarified. As already shown, risk assessments usually refer to the likelihood that a certain event leads to harm to a specific object of protection and to the severity of the harm. In data protection law, these two components make it possible to combine quantitative or at least empirical methods for assessing the likelihood that an event will lead to harm with a qualitative-normative approach for assessing the severity of this harm to a specific object of protection. This means that with respect to the aforementioned tiered protection


24 See in the 1st part at point II. 2. b) The protection of autonomy as such is too vague as a legal scale, referring to Nissenbaum, amongst further authors, Privacy in Context, 13 and 73 et seq.

25 Cf the Human Dignity protected under Article 1 ECFR, which is inherent in all other fundamental rights of the Charter, Jarass, EU Charter of Fundamental Rights, (C.H.Bock, 2016) Art 1, cip 2-5.

system, while in the case of an unspecified risk (i.e. in the precautionary stage), the focus is on assessing the likelihood of whether an event might cause harm at all (i.e. whether an unspecified risk might turn into a specific risk or even harm), the focus shifts equally to the severity of the potential damage (because the specific object of protection is now identified) and to the question of how harm can be prevented at the moment when the risk to a specific object of protection is identified.

In conclusion, the concern that the application of methods and concepts from risk regulation would lead to rabulistic number games and undermine the normative substance of data protection law is therefore unjustified in two respects: First, as far as unspecified risks are concerned, the concepts behind the precautionary principle actually aim, as shown previously, at avoiding the question of whether (and how) a risk can and must be proven by using scientific methods. And second, as far as specific risks are concerned, the direct reference to the other fundamental rights that are specifically concerned ensures that the normative substance of the variety of all these rights stays in the center of the (specific) risk assessment. Thus, the concerns about rabulist number games vanish into thin air as soon as the concept of a “risk to a right” is assessed more precisely on the grounds of (meanwhile quite elaborate) concepts of data protection risk regulation than before. In fact, given the extremely strong focus of the proposed data protection risk assessment methodology on rights, I think the real question is rather which empirical element actually plays an important role for the assessment? In particular, which empirical element may help assess the likelihood that an unspecified risk turns into a specific risk or even harm? What are reliable indicators for this assessment? These questions lead us to the function of the principle of purpose limitation.

2. Regulating Data Collection and Use by the Purpose Limitation Principle

Within the proposed data protection risk assessment methodology, the principle of purpose limitation plays an essential role because the principle functions as a key indicator for assessing whether the data processing causes only unspecified risks to autonomy, or also more specific risks to autonomy guaranteed by one or more of the other data subject’s fundamental rights. Of course, the specification of the purpose is not the only indicator of whether there is a specific or an unspecified risk. If the controller specifies its purpose incorrectly, e.g. does not correctly indicate the real risk caused by its processing to a data subject’s fundamental right, it is still possible to assess the real specific risk on the grounds of further circumstances of the case (in particular the nature of the data, the context and technical means of the processing).27 However, the purpose of a controller is the key indicator to demonstrate first and foremost a causal link between the data processing and harm to a data subject’s autonomous exercise of fundamental rights since the purpose is a very common means to express an intention to reach a future event.28 Thus, if the law requires a controller to indicate the specific risks caused by its data processing to a data subject’s fundamental right by formulating its processing purpose accordingly, the specification of such a (“risk to a right” by a) purpose constitutes the necessary proof that the processing is likely to cause real harm (to this right). Thus, linking first and foremost to the purpose of the controller and not to the context of the processing not only extends the range of protection to an earlier stage, but also provides a reliable indicator of when a controller may specifically harm the autonomy of a data subject.

a. Purpose Specification: Discovering (Differentiating) Specific Risks (from Unspecific Risks)

According to this understanding, the first component of the principle of purpose limitation requires the controller to discover specific risks caused by its data processing against the data subject’s autonomous exercise of fundamental rights. If the controller discovers a specific risk to one or more of the data subject’s fundamental rights, the controller must implement the appropriate (data) protection measures to reduce the risk to a level where this “risk to a right” does not (any longer) outweigh the controller’s own fundamental rights. The variety of all fundamental rights of the data subject thus determine in which

27 Cf EDPB, Opinion 03/2013 on ‘purpose limitation’, 19.
28 See EDPB, Opinion 03/2013 on purpose limitation, 15-16.
way and how precisely a controller must specify its processing purpose: The greater the risk caused by its processing to one or more of the data subject’s other fundamental rights, the more specific the controller must make that risk clear by formulating its purpose accordingly.\(^{29}\) To specify the risk, the controller may have to describe, amongst other aspects, in what context what data is collected and how the data is used, eventually, against the data subject, and by whom.\(^{30}\)

On the basis of such a refined concept of protection, there is no “glaring loophole” that leaves the specification of the purpose to the full discretion of the controller.\(^{31}\) Since the law requires the controller to indicate the risk by its purpose correctly, the controller must do this to legalize its processing. If the controller does not specify the (risk by its processing) purpose correctly, the real risk can be retrospectively assessed by referring to the context of the processing, the type of data etc.\(^{32}\) The intensity of this legal violation depends then on the real risk with respect to the implemented measures: If a controller does not correctly specify a risk through its purpose but implements the appropriate protection measures, this conflicts with Art. 8 sect. 1 and 2 sent. 1 ECFR\(^ {33}\) – but a violation of this right per se does not necessarily outweigh the controller’s own fundamental rights.\(^{34}\) If, on the other hand, the controller does not even implement the appropriate protection measures in the first place, this additionally collides with the other fundamental rights of the data subject – and in sum, the risks together are more likely to outweigh the controller’s fundamental rights.\(^{35}\) In any case, the variety of all a data subject’s fundamental rights provide an objective and nuanced scale that helps to determine both how a controller must specify its purpose and the other appropriate protection measures.

b. Purpose Compatibility: Controlling Specific Risks that Add to the Previous Ones

On this basis, the second component of the purpose limitation principle requires the controller to control those risks that are caused by a change of purpose and add to the risks that have been specified by the original purpose. If this assessment identifies a new risk (i.e. a risk not previously present) from the change of purpose, this is a substantive change of purpose.\(^{36}\) In this case, the controller must again apply the appropriate protection measures (e.g. find the appropriate legal basis, inform the data subjects, implement organisational and technical measures, and so on). Indeed, there may be differences in the need for protection depending on the type of the new risk. For example, if a re-specified purpose “only” reveals a higher risk for the same object of protection than concerned before, the requirements may be lower than if a re-specified purpose reveals a risk for another object of protection that has not been concerned before.\(^{37}\) In any case, only if the controller correctly re-specifies the risks and reduces them by imple-

---

29 Several authors are of the opinion that the purpose must be more precise, the more the data subject is affected, but usually these authors left open how to assess whether a data subject is affected and, if so, how intensively, see for example, Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, *The Principle of Purpose Limitation and Big Data* (Springer, 2017) 31; Marion Albers, “Treatment of Personal Information and Data” in Wolfgang Hoffmann-Riem, Eberhard Schmidt-Aßmann and Andreas Voßkuhle (eds.) *Grundlagen des Verwaltungsrechts, Band 2 – Informationssicherung, Verwaltungsverfahren, Handlungsvorschriften* (C.H. Beck, 2012) cip. 124.

30 ibid, Forgó, Hänold and Schütze.


32 EDPB, Opinion 03/0213 on purpose limitation, 2 April 2013, 00569/13/EN, WP 203, 19.

33 See the method of Bieker et al., according to which any data processing is already a violation of the data protection basic right. Bieker et al., ‘Die Risikobeurteilung nach der DSGVO’ (2018) 8 DuD, 492–496.

34 See EDPB, Opinion 03/2013 on ‘purpose limitation’, 19, in (n 50), where the Board clarifies that further legal consequences, such as a ban of the processing operation, may add to the mere obligation to re-formulate the purpose correctly, but the Board does not explain upon which factors such additional consequences may depend.

35 Cf for example, ECJ C-131/12 (Mr. González vs. Google Spain), cap. 97, where the Court did not only refer to Article 8 ECFR but, in addition, to the claimant’s right to private life under Article 7 to justify the outcome of its balancing exercise where (only) both rights together ‘override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having [... ] access to the information in question.’

36 Cf EDPB, Opinion 03/0213 on purpose limitation, 2 April 2013, 00569/13/EN, WP 203, 21 and 22, which does not explain what the difference between a substantive and a formal change of purpose actually is.

37 Cf Bart Caster and Helena Ursic, ‘Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection’ (2016) International Data Privacy Law, who call these two types “re-purposing” and “re-contextualisation”.
menting the appropriate measures to such an extent that these “risks to a right” no longer outweigh the opposing fundamental rights (in particular of the controller but also third parties and the public), is the processing lawfull.

At this moment, it is time to ask whether the second component of the principle of purpose limitation, i.e. the limitation of subsequent processing of personal data to the original purpose, is a precautionary measure to reduce unspecific risks or a protection measure that controls specific risks. The answer depends on its implementation: If the purpose limitation principle was interpreted narrowly, i.e. requires the purposes to be identical, the principle served to reduce (or even exclude) any unspecific risk that the data might one day be misused – because nobody is allowed to use the data for any other purpose. In contrast, if one requires a purpose compatibility assessment, the principle serves to control specific risks. The reason for this is that the purpose compatibility assessment applies to the moment of the current data processing and use of the retrieved information. Thus, the compatibility assessment expands the control from the moment of data collection to the use of the data or retrieved information. This is often overlooked when authors praise the flexibility of the compatibility assessment by warning, at the same time, of a regulation of data use (instead of data collection).

Interestingly, this understanding of the second component of the purpose limitation principle as controlling specific risks (instead of excluding unspecific risks) is supported by Article 8 ECFR because it is not mentioned in Article 8 ECFR. Article 8 sect. 1 ECFR only refers to the first component of the principle, i.e. that “data must be processed (...) for specified purposes”; it says nothing about the second component that the processing of personal data must be limited to the original purpose. This is where the EDPB is not really clear. However, the interesting fact is that this second component does not have to be mentioned in Article 8 ECFR because it results from the interplay of the first component with the other fundamental rights. Article 8 ECFR as an autonomous right, which serves the protection of the other fundamental rights, is indispensable only as long as the other rights cannot protect themselves. This is the case when their scope does not yet apply (because it cannot yet be sufficiently demonstrated that the data processing causes harm to them) – but an early precautionary protection is needed to avoid early enough that an unspecific risk turns finally out to actually harm them. In contrast, when another right applies, this specific fundamental right determines whether this new (‘risk to a right’ specified by the) purpose is compatible with an eventually preceding risk (to this and/or another right, as specified by the preceding purpose/s). This is only possible, of course, as long as one understands the second component of the purpose limitation principle as a protection instrument that controls specific risks in the moment they arise. If, instead, one understands the second component of this principle as an instrument designed to exclude all unspecific risks, it must be based within Article 8 ECFR – but, as we know, this is not the case. This is why Article 8 ECFR speaks in favour of the specific risk-control approach of the compatibility assessment, without even mentioning it.

c. Precautionary and Preventive Measures to Make it Work

Now it is time to briefly sketch out the other precautionary and preventive measures that are necessary to protect the data subjects against unspecific and, eventually, specific risks. First of all, the effectiveness of such protection – which shifts control from the moment of collection to the moment of data use – requires, in addition to the need to specify the purpose, another tightly connected precautionary measure: The controller must document the original purpose for which it collects the data and all new purposes if these are substantially different. Such a documentation obligation ensures that the controller and/or third parties are able to compare the purposes and thus carry out the compatibility assessment. Thus, the controller must describe whether a specif-

---

38 See, for example, EDPB, Opinion 03/2013 on purpose limitation, 2 April 2013, 00569/13/EN, WP 203, 11, and EDPB, Statement on the role of a risk-based approach in data protection legal frameworks, 30 May 2014, 14/EN, WP 218, 2 et seq.
39 See EDPB, Opinion 03/2013 on Purpose Limitation, 10, stating that “[t]he Charter clearly establishes the principle of purpose limitation”, then adding, of course, that the Charter specifies ‘that personal data must be processed ‘fairly for specified purposes’.”
40 Still unclear about this, Max van Grafenstien, The Principle of Purpose Limitation: The Risk-Based Approach, Legal Principles and Private Standards as Elements for Regulating Innovation (Nomos, 2018) 490 et seq.
ic fundamental right is concerned and, if so, which one and why. In doing so, the controller may have to refer also to the other “analytical instruments”, such as the type of data and/or the context in which it intends to collect the data, and/or re-use it and so on. However, if the processing does not specifically concern another right – for example, because the collected data might be about a data subject but does not reveal sufficient relevant aspects about their private life, and the controller only uses the data for statistical purposes – the controller should, however, describe the actual circumstances of the processing. The reason for this lies in the precautionary approach of Article 8 ECFR: The processing of personal data constitutes the “reason” that the processing might affect the autonomous exercise of the data subject’s further rights.43 By describing these circumstances, the controller can demonstrate that these concerns are unjustified and, therefore, there is no need for additional safeguards against specific risks.

This leads to the result that if a data controller (or a user of information) cannot demonstrate where the data comes from (i.e. the risk that the processing has caused so far; and if there was no risk, why not) on which its processing is based, the controller is not allowed to process the data or use the information. The reason for this strict approach is that if a controller does not know what the original purpose was, it can only assess the current risk, but it cannot find out whether there is a new risk that adds to the previous risk. Whether there is a new risk adding to the previous one, however, is decisive because the data subjects may not have given their consent or not have concluded the contract or not used the service if they had known that this would lead to this (new) later risk. Thus, without knowledge about the original purpose (or previous purposes), the controller cannot carry out the purpose compatibility assessment and, therefore, may not carry out the processing. Again, the reason for this strict result is in the precautionary approach of Article 8 ECFR, which shifts the burden of proof (i.e. that the processing does not cause a specific risk to the data subject’s other fundamental rights) to the controller. However, it should be clear that this does not mean that this approach prohibits processing per se, which would likely be disproportionate.42 Instead, the approach requires the controller to document its purpose, only; and only if the controller does not do so is this not allowed. Thus, it is in the hands of the controller to create the conditions for the legality of its processing. Such a formal requirement is proportionate as the formalisation of the controller’s knowledge corresponds to the formalisation of the data processing per se. Thus, in this regard, the documentation requirements are ultimately just the price that the controller has to pay in turn for its increased informational power by the data processing.43 This in turn means, of course, that the less formalised and structured the data processing, thus, the less informational power asymmetry, the easier such obligations must be.44

Besides these obligations to document the purpose, there are further precautionary measures that are necessary to avoid the unspecific risks becoming specific and resulting eventually in harm. Again, as long as the purpose does not indicate specific risks against the other rights, there will of course always remain the unspecific risk that the data could later be used in a way that creates a specific risk or even harm to one (or more) of the other fundamental rights. Against these remaining unspecific risks, the data controller, as well as the processor – i.e. any entity that gets in contact with personal data, regardless of the current purpose – must implement precautionary measures that unauthorised persons cannot access and misuse the data, i.e. implement the appropriate IT security.

Last but not least, another precautionary measure is transparency as long as this is necessary to counteract unsettling speculations of the data subjects about what may be done with the information about them, i.e. their pure “feeling that their private lives are the subject of constant surveillance”,45 or in other words their “unspecific Angst” that another entity might have some information about them without knowing what the precise information is and what is actually done with that information.46 This precautionary measure requires information about

41 See regarding the concept of the precautionary principle in the 1st part at point III. 2.
42 See in the 1st part at point III. 3. Proportionality of the protection strategy and its instruments.
43 (n 15) 246 et seq.
44 Cf Art 30 5 5 GDPR.
45 Cf ECJ C-293/12 and C-594/12 (Digital Rights), cip. 37, and ECJ C-203/15 und C-698/15 (Tele2), cip. 100.
46 Cf BVerfG, 2nd March 2010, 1 BvR 256/08, 1 BvR 263/08, and 1 BvR 586/08 (Data Retention), cip. 241.
the real processing purpose aka. risk. Only if data subjects know which entities have which information about them and what these entities really do with that information, the data subjects can trust that this information is not “misused” in another manner (than they should expect in view of the transparency offered by the controller/s). In this respect (but only to that extent), data protection exists against the use of personal data, which does not actually take place.\textsuperscript{47} However, as explained previously, the reason for this is the collection of the personal data, according to the concept of precaution. In contrast, if personal data is not even collected, the controller does not have to ensure transparency and the individuals can conclude from this lack of transparency that no personal data is collected. Both cases demonstrate that individuals have to principally trust in the fact that data controller respect the law – and the reason for this trust is the existence of the law itself.\textsuperscript{48}

In addition to these precautionary measures, the data controller must implement preventive measures if its processing purpose discovers a specific risk against another fundamental right. Such a right may primarily be the right to private life in Article 7 ECFR if the data collected and, even more so the analysis of that data reveals information about someone’s private life. It is already a harm to this right to privacy if another person gets access to this information. However, as long as only machines process the data and no human accesses the information, I think that this is only a risk to this right (however, a specific risk because all machines are owned by humans and therefore it is sufficiently likely that the owner of a machine will one day also have access to the information). A prominent preventive measure to reduce this risk is to minimise the information about the data subject (in particular by using anonymisation or pseudonymisation techniques). Another important measure giving data subjects control over this risk is to oblige the controller to obtain the data subjects’ consent when the controller seeks to collect information about them. Data subjects can therefore decide whether to remain private or to disclose themselves, and in fact to whom. Since this right contains several more specific objects of protection (e.g. privacy of one’s family life, privacy of her intimate sphere, privacy in public, privacy of the home, privacy of communications, etc.), these measures may be applied differently depending on the specific legal guarantee. Thus, there may be different legal protection needs in relation to the question of under which circumstances information is seen as “relating to an individual” (e.g. when an individual is “identified”), what information about an identified individual exceeds the threshold for legal protection, or the requirements for the validity of the consent (e.g. through an opt-in or opt-out procedure).\textsuperscript{49}

Another object of protection that is discussed with respect to collected information about an individual is discussed as a “right to unbiased freedom of development”. To ensure that an individual can take part in society and develop his or her personality freely it is argued that she must be able to know to some extent what other people know about her.\textsuperscript{50} The obvious measure to protect such an object of protection, is a right to transparency regarding the information that others have about them.\textsuperscript{51} Of course, following the focus on data, such a right will be limited to information that is somehow formalized. This means, for example, in the case of profiles on a data subject that the data subject needs to know not only the data on which their profile is based (e.g. a certain behaviour when visiting a website), but also the formalised criteria that define his or her profile (such as conclusions about their age, gender and income, and interest in a certain category of products or services).\textsuperscript{52}

While these rights to privacy and unbiased freedom of development are usually affected at the moment when the data are to be collected, other protection objects are typically affected at a later stage of

\textsuperscript{47} See, in this regard, Data Hallinan, ‘Data Protection without Data: Could Data Protection Law Apply without Personal Data Being Processed?’ (2019) EDPL 3, 293 et subseq.

\textsuperscript{48} (n 40) 407 et seq.

\textsuperscript{49} Ibid 361 et seq.


\textsuperscript{51} See Lars Becher, Informationseingriffe durch transparenten Umgang mit personenbezogenen Daten, (Universitätsverlag Halle-Wittenberg, 2010) 20 - 21, as well as 92 et seq.

\textsuperscript{52} Still unclear at Max van Grafenstien, The Principle of Purpose Limitation: The Risk-Based Approach, legal Principles and Private Standards as Elements for Regulating Innovation (Nomos, 2018) 396 et seq.
the data processing, in particular when the information is used to make a decision in favour of or, more importantly, to the detriment of the data subject.53

For example, the data processing could undermine the data subject’s rights to equality, justice, freedom, and so on. In this regard, a major problem is that the underlying data processing could lead to wrong conclusions (that form the informational basis for negative decisions). In particular, the question arises as to whether the mathematical-statistic methods used for a conclusion are justified. A key challenge here refers to the relation of correlation and causality. Causality means that one event leads to another one; in contrast, a correlation only indicates a relation between two events, which may, however, be connected through a third event (or even more).54 Also in this regard, transparency and access rights play a crucial role because they are the precondition for the data subject to react to such a decision, e.g. if not by adapting their behaviour, then by intervening in the decision-making process, such as to contest the validity of the conclusion. An interesting aspect thereby is that such a system does not require the data controller to understand how an algorithm used for its decision-making process actually arrived at its result (i.e. outcome).55 The controller only needs to explain why it (or another party) takes the conclusion seriously and therefore uses the information against the data subject. The data subject can then contest this explanation so that the real reason is actually irrelevant.56 Beside this kind of transparency, further measures are possibilities to correct incorrect data, to complete incomplete data, to propose opposing views, to question the presented logic of the decision-making process, or to object to this process as a whole. With respect to questioning the decision-making process, an appropriate protection measure may consist in a (dispute resolution) mechanism that allows data subjects to challenge a conclusion about their behaviour by reversing the burden of proof on the basis of the information provided. Here again, the concepts of regulating risks can help to capture the problem (i.e. knowledge uncertainties) and the appropriate measures, such as mechanisms that shift and balance the burden of proof, respectively.57

In any case, the aim of these considerations is not to present an exclusive list of rights that can be put at risk by the processing of data nor of the appropriate protection measures. This section should only demonstrate how a more nuanced differentiation between different types of risks and where specific risks arise, the variety of all fundamental rights can help to adjust the appropriate protection measures to the actual need for protection in a specific context.

3. More Effective and Proportionate Protection Through a Multi-Layered System

Even if this concept is more complex than, for example, a simplistic data-determination right, it is, in the end, more proportionate because it creates less regulatory burden for the entities that process personal data and provides data subjects for more effective protection. Some readers might doubt this claim, in particular, whether the proposed understanding of the compatibility assessment implies a shift in control from the moment of data collection to the moment when the data is used.58 In other words, a use regulation rather than a data collection regulation?59 Yes and no: There is a shift in control to the moment when

53 However, see the (re)-publication of personal data as also covered by the right to private life, ECJ C-131/12 (Mr. González vs. Google Spain), as well as the criticism based on a pre-version of the refined concept as proposed in this three-parted contribution at Max van Craenenbtrg Wolfgang Schultz, ‘The Right to be Forgotten in Data Protection Law: A Search for the Concept of Protection’ (2015) 5 International Journal for Public Law and Policy 3, 249–260.

54 See, for example, Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (Houghton Mifflin Harcourt, 2013) 87 – 125; Of course, the concept of ‘causality’ is more complex than that, see for instance, Michael Baumgartner and Gerd Grafheu, Kausalität und kausales Schließen – Eine Einführung mit interaktiven Übungen (Bern Studies in the History and Philosophy of Science, 2004).

55 Understanding the logic of algorithms is increasingly a problem with deep learning techniques, see Jenna Burrell, ‘How the machine “thinks”: Understanding opacity in machine learning algorithms’ (2016) 12 Big Data & Society 1; but also for first technical solutions under <http://heattesting.org>.

56 See the difference between producing and explaining a decision at Niklas Luhmann, Recht und Automation in der öffentlichen Verwaltung (Duncker & Humboldt, 1997, 49 et seq.

57 See in the first part at point III. 2. The risk-based approach and the precautionary principle.


59 See the concerns regarding a regulation of data use instead of data collection, for example, at Chris Jay Hoofnagle, ‘The Potemkinesis of Privacy Pragmatism: Civil liberties are too important to be left to the technologise’ (2014) <http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the libertarian_push_behind_a_new_take_on_privacy.html> accessed 17 June 2020.
the data is used, but this does not mean less control. There is control also in the moment of collection. But control as such does not mean that the controller has to implement all protection measures in the moment of collection at once. In principle, the controller must rather monitor whether the intended data processing poses a specific risk to the other fundamental rights. If there is no specific risk, the controller is relatively free to do whatever it wants with the data. There are a few further precautionary measures to make sure that the data is not subsequently misused (esp. to document the purposes, IT security and information duties to counter unsettling speculations). However, the purpose limitation principle does not require the controllers to limit their subsequent processing to purposes, which they could hardly specify all in advance.

Only if there are specific risks, the controller(s) must implement additional appropriate protection instruments to make sure that the processing does not undermine the data subjects’ autonomous exercise of rights. Thus, the proposed approach stretches the application of the variety of data protection measures over time. This gives more leeway to the controller(s) to react accordingly over (and in) time, rather than focusing solely on the moment of data collection. This also makes protection more effective for the data subjects, because, for example, they receive the necessary information together with their rights of intervention (i.e. consent or objection to the processing, correction or deletion of the data, and so on), when these are relevant. Of course, many measures, especially of transparency, serve to protect not only against one type of risk but can also protect several objects of protection. However, the proposed concept makes it possible to adjust much more precisely the multitude of protection measures, yes, even one single protection measure to the multitudes of specific normative needs in a specific data processing context. This makes the proposed tiered system more proportionate.

IV. Why Article 8 ECFR is Indispensable with Respect to the Other Fundamental Rights

Interestingly, the proposed refinement of the object and concept of data protection does not only lead to a more proportionate protection but can also explain why Article 8 ECFR is “indispensable” in relation to the other rights. On this basis, this chapter clarifies few further aspects regarding a regulation of data protection risks on the level of fundamental rights.

1. Protection of the Other Rights Before Their Own Scope Applies

The first reason for this is that the right to data protection protects the other rights before their own scope applies. Thus, there must be another right that provides such a precautionary protection. Indeed, one could say that such precautionary protection could also be provided by the right to private life under Article 7 ECFR. The right to private life usually applies in the moment of collection of the data and therefore often (and sometimes even long) before the data is used in a way that undermines the autonomous exercise of other fundamental rights. But not all personal data may reveal (sufficiently relevant) information about the private life of a data subject. This may be the case, for instance, because the data has not yet turned into information or because too much additional knowledge is needed to identify a person. The “purpose” element also illustrates that the data may relate to a person because the controller uses the data to treat the person in a specific way, without necessarily revealing information about that person. Thus, there is a certain need for precautionary protection regarding the processing of data that does not necessarily fall under the right to private life.

Furthermore, the object and concept of an individual’s right to private life is not consistent with the need for protection under the other fundamental rights. The right to private life guarantees that an individual is able to be left alone and can decide when to disclose themselves to others and under which conditions. The scholars De Hert and Gutwirth call the respective measures of protection “tools of opacity.” In contrast, Article 8 ECFR protects data subjects against the risk that the personal data processing un-

62 See above at point III. 2. c) Precautionary and preventive measures to make it work.
63 See Paul De Hert and Serge Gutwirth, ‘Privacy, data protection and law enforcement. Opacity of the individual and transparency of power’ in Erik Claes et al (eds.) Privacy and the criminal law (Intersentia, 2006) 61-104.
dermines their autonomous exercise of other rights. This risk arises in particular, when data are used in contexts other than that in which they were collected. Thus, the most urgent need for protection requires an instrument that controls the flow of the personal data across varying contexts and, therefore, mechanisms to detect new risks arising from such a change in context, such as transparency and intervention rights. On the one hand, it seems therefore more feasible to bundle and orchestrate these procedural measures (as well as the methodical knowledge about their effectiveness etc.) under one fundamental right that supplements and supports the other more substantial fundamental rights than to allocate these measures under each specific right, respectively. On the other hand, allocating this right under the right to privacy automatically grounds its concept of protection in the privacy logics. However, such a grounding quickly leads back to a data determination-right, which enables the data subjects to decide not only on whether information about them is collected but also how this information is used. In contrast to such “tools of opacity” of the right to private life of the data subjects, the function of the right to data protection is, indeed, structurally different.64

2. Why Precautionary and Preventive Protection Must Complement Each Other

The preceding considerations also make it clear why the approach of limiting the scope of the right to data protection to the precautionary stage does not really work. At the very least, understanding the right to data protection purely from the angle of the precautionary principle alone would not solve the problems as proposed. If the right to data protection provides protection only against unspecific risks, but not against specific risks for the other rights, all the discussed problems will reappear: What then is the objective and differentiating scale that allows to assess the data protection risks and the appropriate protection measures? How then to specify the purpose and assess whether new purposes are not incompatible with the original purpose? And how can one then reliably define in which context the data may be used and under which conditions? In contrast, if one adds to the precautionary approach the risk-based approach that also protects against specific risks to the other fundamental rights, such kind of protection is not only more effective but also more proportionate, as has been shown before.65

3. A Subjective Right to Control Processing Risks in the Constitutional Order

Last but not least, there are a few aspects that should be clarified with respect to the proposed concept of regulating data protection risks on the level of fundamental rights. Instead of controlling data, the proposed concept of protection argues that an individual has a right to control the data processing risks to their autonomous exercise of fundamental rights. To this extent, data subjects have a subjective right to control these risks66 – the wording of Article 8 sect. 1 ECFR makes this very clear67 – and such a subjective right does not only apply to the protection against specific risks to the other fundamental rights, but also to the precautionary stage. Data subjects hence have a fundamental right to be sure that the controller specifies its purpose and applies the other precautionary measures (esp. documentation, transparency and IT security), correctly.

In contrast, even if the right to data protection also serves as a precondition for a democratic civil society,68 the data subject has no subjective right to protection of abstract constitutional principles, such as the principle of democracy. If the processing of personal data causes a risk to such a principle, this might be considered only as a factor in the balancing exercise that intensifies the infringement of an individual’s subjective right.69 An example of political microtargeting may illustrate this thought: while data

64 ibid.
65 The cutting back of the scope of protection of the right to informational self-determination to the precautionary stage by the German Constitutional Court is the overlooked design flaw of its recent decision at BVerfG, 06th November 2019 - 1 BvR 16/13 (Recht auf Vergessen I), especially cip. 85.
66 See to the contrary, Nikolaus Marsch, Das europäische Datenschutzrecht (Mohr Siebeck, 2018) 203 et seq (who, actually, for the most part only transfers Albers’ concept to the ECFR).
67 ‘Everyone has the right to the protection of personal data concerning him or her.’
68 (n 63) 61-104.
69 Dietlein, Johannes, Die Lehre von den grundrechtlichen Schutzpflichten (Berlin Duncker & Humboldt, 2005), 104 and 105
subjects have a right to data protection with respect to their autonomous exercise of their right to vote according to Art. 39 and 40 ECFR (i.e. not being manipulated in their vote by means based on the processing), they cannot require the controller to implement measures maintaining a public political debate (to counterfeet the collective risk that the public debate falls apart into a myriad of micro-debates). However, the controller could take such measures in order to introduce them as a factor in the balancing exercise, reducing the intensity of the voters’ data protection right. Of course, beside such a solution provided for by the controller, the regulator can establish such duties on the basis of public law, i.e. first and foremost in the public interest.

V. Outlook: Consequences for the Interpretation of the GDPR

On the basis of the proposed refined object and concept of Article 8 ECFR, the third and final part of this three-parted series will finally draw several conclusions for the interpretation of the GDPR. In particular, the third part will focus on the following aspects: First, the actual room for maneuver of the EU legislator transposing the proposed concept for Article 8 ECFR into ordinary law (especially the GDPR). Second, the implications for interpreting the principle of purpose limitation with particular respect to the legal basis (Art. 5 sect. 1 lit. a and b and Art. 6 sect. 1 and 4 GDPR). Third, the phenomenon of the multitude of overlaying risk assessments, beginning with the assessment on an abstract-general basis conducted by the legislator to the variety of individual-specific risk assessments that the controllers and processors have to carry out (when applying the legal norms). Fourth, the possibility to make these risk assessments scale. The three-parted series will conclude with an outlook on further ambiguities to be clarified.