This final manuscript is for academic purposes only. Please do not circulate without the author's permission, and always refer to the published version:

"On boundaries. Finding the essence of the right to the protection of personal data." in Leenes, Van Brakel, De Hert and Gutwirth, *Privacy and Data Protection: The Internet of Bodies*, Hart Publishing (2018).

On boundaries - finding the essence of the right to the protection of personal data

Abstract: In this contribution, I identify the essence of the right to the protection of personal data as understood in EU law. The essence is a fundamental step in defining the permissible limitations of the right; it works as a theoretical border, the trespassing of which leads to the automatic violation of the right. I claim that, in order to find the essence, it is first of all necessary to trace the contours of the right to the protection of personal data. In its case law on the protection of personal, the CJEU has hitherto followed a susbstantive approach to the essence of Article 8 of the Charter withouth, however, providing indications on how it reached its conclusions. I therefore supplement the scant case law of the CJEU with work on indicators developed by the OHCHR, which provides a method for identifying attributes of rights from which I distil the essence. While the final definition of the essence largely depends on the findings of the CJEU, nevertheless this does not imply that discussing the essence is taboo. This is because defining, even if temporarily, the content of the essence and related attributes has relevance beyond the courtroom. The proposed attributes and essence can help in gaining granularity when analysing the intrusiveness of technologies on the right to the protection of personal data (and other rights), and support data protection by design approaches.

1 Introduction

The protection of personal data has come a long way and is finally acknowledged as a(n almost completely independent) right enshrined in Article 8 of the Charter,[1] which reads:

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

As with all other rights enshrined in the Charter, the right to the protection of personal data must be read in the light of the Charter's horizontal clauses, which command that the essence of the right(s) be respected. The purpose of this article is to shed light on the notion of

[1] *Charter of Fundamental Rights of the European Union, Oj C 303/01*, Official Journal C 303/1, (14 December 2007).

the 'essence' of the right to the protection of personal data. It asks why the essence matters, what it is, whether and how it can be identified.

Such an operation is not as surgical as it may appear: the notion of essence is far from being clear, and the Court of Justice of the European Union (hereafter CJEU) has thus far not committed to a single approach. Furthermore, looking for the essence, or core areas, of the right begs the question as to what constitutes the peripheries of that right – i.e. tracing its boundaries. Such an operation is both unprecedented and temporary. The latter is due to the fact that our understanding of the right is in a state of (fast-paced) flux dictated by the evolution of the technology underpinning the collection of personal data. Yet, the discussion of the essence is also supported by well-established theoretical debates, because the right to the protection of personal data is of statutory origin[2] and was born as a bundle of principles, the so-called fair information principles or FIPs.

The chapter develops as follows. In section 2 I expound the notion of the essence in the Charter, as well as its theoretical origins. Furthermore, I present two approaches followed by the CJEU with respect to the essence in the case law on Art. 8 of the Charter. In section 3 I engage with the literature addressing, directly or indirectly, the essence of the right to the protection of personal data and the logically preceding step, i.e. the attributes, of the right, and I propose a method to identify both attributes and essence. In section 4 I explain the steps needed to find the attributes and essence of Article 8 of the Charter. Section 5, which is the most substantial, is devoted to the illustration of the attributes and essence; I conclude section 5 with some considerations on the role of sensitive data. After summarising my findings, in the conclusions I discuss the advantages and limitations of identifying the attributes and essence, I identify the potential addressees of this exercise, and engage with the ultimate question of why we should safeguard the right to the protection of personal data.

2 The essence in EU law: rationale, nature and how to find it

2.1 THE ESSENCE IN ART. 52(1) OF THE CHARTER AND IN THE LITERATURE

The answer to the question 'why does the essence matter' can be found in article 52(1) of the Charter, which is the horizontal clause on permissible limitations to all qualified rights contained therein, such as the right to the protection of personal data:

> *"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 (...)"*

The Explanations[3] clarify that limitations must be interpreted restrictively and cannot "constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights".[4] So, while the formulation of Article 8 would allow for the application of a margin of appreciation, on the other hand respect for the essence

[2] Lee A. Bygrave, *Data Privacy Law. An International Perspective* (Oxford: Oxford University Press, 2014).
[3] *Explanations Relating to the Charter of Fundamental Rights, Oj C 303/02 (Explanations to the Charter)*, (14 December 2007).
[4] Judgment of 13 April 2000 in Karlsson and Others, C- 292/97, EU:C:2000:202, para 45 (2000).

is deemed to be stringent.[5] In other words, a violation of the essence of the right would be impermissible, i.e. it would be contrary to the rule of law upon which the Charter, and the EU public policy (ideal *ordre public*), rely.

This begs the question of the nature of the essence and, further down the line, how to identify it. The notion of essence contained in the Charter originates from German law,[6] where it is tied to dignity.[7] Brkan[8] argues that the codification of the essence in EU law constitutes a general principle stemming from the constitutional traditions of at least eight Member States, that it is rooted in the ECHR (Art. 17) and the case law of the Strasbourg Court, and that it is echoed by early case law of the CJEU, such as *Hauer* (C-44/79), where the Court used the similar notion of the "very substance" (which is also mentioned in the Explanations to Art. 52 of the Charter).

According to the literature surveyed by Brkan,[9] scholarship looks at the essence either in relative or absolute terms. According to the former approach, which she calls integrative, the essence only bears declaratory nature, and can be subject to a proportionality test. For instance, in Alexy's[10] theory of rights, the idea of 'essence' or 'cores' breaks the stalemate that may derive from a pure application of balancing (proportionality). This could be the case when two equally important principles collide, and their relational interference is equally serious. Moreover, although judicial decisions are informed by uniform legal principles, the weight applied to each principle often depends on the right at stake. In a pure balancing scenario, such a clash of principles could only be solved by elevating one set of values above another, with the consequence of engendering a reductionist view of rights that unjustly sacrifices the idea of their classic interrelatedness.[11] The inclusion of 'nuances' avoids such a reductionist view of rights, by supplying additional layers of analysis.

Conversely, the latter approach, which she dubs exclusionary, sees the essence as a limit which cannot be crushed, and cannot therefore be subjected to a proportionality test. An example of the latter is Scheinin's[12] reinterpretation of Alexy's theory of rights. According to him, a violation of the core, or essence, entails the impermissibility of a limitation (and therefore precludes the further application of the test for permissible limitations). The essence is to be seen as a metaphor, in that fundamental rights may hold multiple cores "defined through a multitude of factors" and "not preventing contextual assessment."[13]

---

[5] Paul Craig, *The Lisbon Treaty, Revised Edition: Law, Politics, and Treaty Reform* (Oxford: Oxford University Press, 2013).

[6] Ibid.

[7] Maja Brkan, "In Search of the Concept of Essence of Eu Fundamental Rights through the Prism of Data Privacy," in *Maastricht Working Papers, Faculty of Law 2017-01* (2017), p. 14. She notes this is further demonstrated by Art. 1 and related Explanations. "The Concept of Essence of Fundamental Rights in the Eu Legal Order: Peeling the Onion to Its Core," *European Constitutional Law Review*, no. 2 (2018 (forthcoming)).

[8] "In Search of the Concept of Essence of Eu Fundamental Rights through the Prism of Data Privacy," pp. 6-12. "The Concept of Essence of Fundamental Rights in the Eu Legal Order."

[9] "The Concept of Essence of Fundamental Rights in the Eu Legal Order."

[10] Robert Alexy, "Constitutional Rights and Legal Systems," in *Constitutionalism - New Challenges: European Law from a Nordic Perspective*, ed. Joakim Nergelius (Brill); ibid.

[11] As discussed, for instance, in United Nations, International Human Rights Instruments, "Report on Indicators for Monitoring Compliance with International Human Rights Instruments," in *HRI/MC/2006/7* (2006), p. 3.

[12] Martin Scheinin, "Terrorism and the Pull of 'Balancing' in the Name of Security. Law and Security, Facing the Dilemmas," in *European University Institute Law Working Paper 11* (Florence2009).

[13] See Scheinin in Maria Grazia Porcedda, Mathias Vermeulen, and Martin Scheinin, "Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project," (Florence: European University Institute, 2013), pp. 43-44.

2.2 THE ESSENCE IN THE CJEU CASE LAW ON ART. 8

Brkan rightly notes that, in its case law, the CJEU "unjustifiably ignore[s]"[14] making use of the test of the essence, with the notable exception of *Schrems*,[15] the first case ever to be solved, though not without criticism,[16] solely on the basis of the essence. Nevertheless, according to Brkan, the few cases adjudicated on the basis of the essence (or the coterminous notion 'very substance') suggest that the CJEU follows an exclusionary approach.[17]

Unfortunately, the case law on Article 8 of the Charter does not offer hints in either direction, because the essence of data protection has not been found by the CJEU to have been breached yet. Nonetheless, the Court has made reference to the essence in four cases relating to the protection of personal data yielding lessons of relevance for this research. In the first and less famous case of *Coty,*[18] the Court found the implementation of Art. 8 of the Charter to be affecting the essence of other rights (so this is not, strictly speaking, a case on the essence of Art. 8). In the aforementioned *Schrems*, the Court found the lack of implementation of rules stemming from Art. 8 of the Charter to be impacting on the essence of another right. As for the other two cases, *Digital Rights Ireland*[19] and *Opinion 1/15,*[20] the CJEU identified substantive elements of the essence of Art. 8 of the Charter.[21] I analyse the four cases in chronological order.

2.1.1 Coty: procedural approach to the essence

Coty, which resulted from a request for preliminary ruling adjudicated by the Court in 2015, concerns the reconciliation of the protection of personal data with the rights to an effective remedy and to property (enshrined in Articles 47 and 17(2) of the Charter) (§33). The case referred to proceedings between Coty Germany GmbH, a company which owns intellectual property rights, and a banking institution, the Stadtsparkasse Magdeburg. The dispute concerned the refusal of the Stadtsparkasse to provide Coty Germany GmbH with information relating to a bank account, i.e. personal data, necessary to identify a person responsible for the sale of counterfeit goods infringing the intellectual property rights of Coty Germany. In this case, the Court interpreted the requirement of the essence stemming from Article 52(1) of the Charter as meaning that permissible limitations cannot result in a serious infringement of a right protected by the Charter for the sake of fulfilling another right protected by the Charter (§35). Following this reasoning, the CJEU found that a "national provision which allows, in an *unlimited and unconditional manner*,[22] a banking institution to invoke banking secrecy in order to refuse to provide, pursuant to Article 8(1)(c) of the Directive 2004/48/EC, information concerning the name and address of an account holder" (§37) is "liable to frustrate the right to information recognised in Article 8(1) of Directive 2004/48 and

[14] Brkan, "In Search of the Concept of Essence of Eu Fundamental Rights through the Prism of Data Privacy," p. 13.
[15] *Judgment of 6 October 2015 in Schrems, C-362/14, ECLI:EU:C:2015:650* (2015).
[16] "In Search of the Concept of Essence of Eu Fundamental Rights through the Prism of Data Privacy," p. 16-17; "The Concept of Essence of Fundamental Rights in the Eu Legal Order."
[17] "The Concept of Essence of Fundamental Rights in the EU Legal Order."
[18] Judgment of 16 July 2015 *in Coty Germany, C-580/13, ECLI:EU:C:2015:485* (2015).
[19] Judgment of 8 April 2014 in *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238 (2014).
[20] Opinion 1/15 of the Court (Grand Chamber), ECLI:EU:C:2017:592 (2017).
[21] Note that *Tele2Sverige* does not figure in this list. Unfortunately the CJEU did not follow the suggestion given by the Advocate General Saugmandsgaard Øe in an *obiter dictum* of his Opinion; see further, sections 3.1 and 4.1.
[22] Emphasis mine.

is therefore [as follows from paragraph 29], such as to infringe the fundamental right to an effective remedy and the fundamental right to intellectual property" (§38). This is capable of seriously impairing the effective exercise of the right to intellectual property" (§40).

This approach to the essence of rights in general can be dubbed 'procedural', because protecting individuals by withholding their personal data frustrates the exercise of the right to an effective remedy, which is instrumental to enjoying the fundamental right to property (§29).

2.1.2 Digital Rights Ireland: substantive approach to the essence

Digital Rights Ireland concerns the reconciliation between Article 8 (and 7) of the Charter with the objective of general interest of public security. The case stemmed from a joint request for preliminary ruling raised by the Irish High Court and the Austrian *Verfassungsgerichtshof* concerning proceedings challenging the compatibility of the Data Retention Directive (24/2006/EC) with the rights enshrined in article 8 (and 7) of the Charter. In order to appraise the compatibility, the CJEU developed a fully-fledged test pursuant to Art. 52(1). First, the CJEU ascertained that there was an interference with the rights (§ 35-36). The Court skipped the legality test, in the clear presence of a legal basis, and it assessed whether the interference represented by the Data Retention Directive impinged on the essence of the right (§ 39-40). In that context, the Court elaborated, *a contrario*, a substantive understanding of the 'essence' of article 8

> *"(Nor is that retention of data such as to adversely affect) the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that ... Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data."(§40)*

As well-known, the Court struck out the Directive on the basis of its threefold lack of limitedness (non-excessiveness) *vis-à-vis* what is strictly necessary to attain the Directive's objectives (§57, 60 and 63), rather than on the basis of the violation of the essence of rights (§48). This is somewhat in contrast with the fact that the CJEU found that the very same provisions of the Directive fulfilling the essence do not "ensure that a particularly high level of protection and security is applied '… by means of technical and organisational measures" and the fact that those data could be retained outside the EU hinders "compliance with the requirements of protection and security" (§67-68). In sum, the Court identified the essence of Article 8 in data security, which would be fulfilled by the presence of minimum provisions in the applicable law; the assessment of the quality of those provisions was left to the proportionality test, the result of which is that the quality of the law was sub-standard.[23]

2.1.3 Schrems: 'essential components' (and missed opportunities?)

[23] This seems closer to what has been termed the integrative (relative) approach to the essence, as opposed to the exclusionary (absolute) approach discussed, and supported, by Brkan. Brkan, "In Search of the Concept of Essence of EU Fundamental Rights through the Prism of Data Privacy," p. 22; "The Concept of Essence of Fundamental Rights in the Eu Legal Order." Note that it is beyond the scope of this chapter to take sides on this debate.

In *Schrems* the Court invalidated Decision 2000/520, pursuant to which the Safe Harbour Agreement was deemed adequate, because the Agreement impinged on the essence of Articles 7 and 47. The Court found the violation of the essence of the right to an effective remedy (Art. 47) to stem from the absence of provisions in the applicable law expressing data subjects' rights, namely "for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data" (§95). *A contrario*, elements of the protection of personal data appear to constitute the essence of the right to an effective remedy, but not the essence of Article 8. This approach is problematic, in that it seems to negate the interrelatedness and interdependency of Art. 8 and 47, which overlap, as they both express elements of the rule of law (see further section 5.2). Arguably, the approach followed by the Court in *Coty* could have led to confirm such interrelatedness.

The case further raises an important terminological question. In §41, the CJEU said

> *"The establishment in Member States of independent supervisory authorities is therefore (...) an essential component of the protection of individuals with regard to the processing of personal data" (§41).*

This quote raises the question as to whether the locution 'essential component' of the right is equivalent to the 'essence'. Three facts constitute arguments against such equivalence: first, 'essential component' is discussed at the beginning of the judgment, as part of the preliminary considerations; second, the quote refers to the wording of Recital 62 of Directive 95/46; and thirdly, the CJEU did not explicitly choose to use 'the essence', as it did instead for Articles 7 and 47.

2.1.4 Opinion 1/15: back to the substantive approach to the essence

Opinion 1/15 was pronounced in response to a request, advanced by the European Parliament, to assess the compatibility of the draft Agreement on the exchange of Passenger Name Record data between the EU and Canada with Art. 8 (and 7) of the Charter (as well as to assess the adequacy of the legal basis pursuant to which the Agreement was adopted). Similarly to *Digital Rights Ireland*, *Opinion 1/15* concerns the reconciliation between Article 8 (and 7) of the Charter with the objective of general interest of public security (§149).
Here the Court confirmed the understanding of the essence found in *Digital Rights Ireland* (though with a slightly different wording), and further expanded it. In detail, in §150 the Court found that

> *As for the essence of the right to the protection of personal data, enshrined in Article 8 of the Charter, the envisaged agreement limits, in Article 3, the purposes for which PNR data may be processed and lays down, in Article 9, rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing.*

The Court identified the essence of personal data in rules ensuring the "security, confidentiality and integrity" (see *infra*, section 5) of data, which protect it against unlawful access and processing. In addition, the Court added to the list (also *a contrario*) the well-known principle of 'purpose limitation'. As in *Digital Rights Ireland*, the simple presence of minimum rules, coupled with the existence of an objective of general interest, entails for the Court an automatic fulfilment of the essence (§150). The Court resolves the case instead by means of a classic proportionality test.

For the purposes of this discussion, what matters is that in the case under analysis (as in *Digital Rights Ireland*), which concerns the clash between fundamental rights and objectives

of general interest, the CJEU identified the essence as a substantive component of the right expressed in secondary law, the omission of which would be impermissible. The extent to which the entitlement expressed in secondary law is implemented can be further appraised by the court in the context of a test for permissible limitations.

2.1.5 Lessons learnt from the case law and open questions

The four cases converge on some matters, but also diverge on others. *Coty* and *Schrems* have in common the denial of a right to an effective remedy. In the first case, rules implementing Article 8 are found to impinge on the essence of the right to an effective remedy and to property; in the second case, it is the absence of rules in the legal standard stemming from Article 8 that is found to impinge on the essence of the right to an effective remedy. In *Coty*, which concerns the reconciliation of fundamental rights, the Court refers to the essence in 'procedural' terms: the essence (and, *a contrario*, permissible limitations) lies in the ability to exercise a right *tout court*, hence it lies in its guarantees, which in fact become fundamental when a right's enjoyment is limited. Differently, in *Schrems*, the CJEU construes elements of Art. 8 as the essence of the right to an effective remedy.[24] Moreover, the Court refers to the 'essential components' of the right, which begs the question of the relationship between this concept and the essence. I will come back to this point in sections 3 and 4, where I discuss the concept of attributes.

In *Digital Rights Ireland* and *Opinion 1/15,* which concern the reconciliation between fundamental rights and objectives of general interests, the Court unambiguously defines the nature of the essence of Article 8 of the Charter in substantive terms. This can be dubbed the substantive approach, whereby permissible limitations must respect the enjoyment of a specific facet of the right, as codified in a legal provision.

In sum, when the Court expressed itself on the essence of Art. 8, it did so in substantive terms. Conversely, the case law on the essence of other rights in relation to Article 8 Charter does not seem to lead to a single approach and leaves several doors open. Ultimately, it is for the Court to clarify which of the approaches is bound to prevail in the case law concerning Art. 8. However, this should not imply that discussing the essence is taboo. Pending a clarification by the Court, I will borrow from the lessons drawn from all four cases to identify candidates for the essence and the logically preceding step, the attributes of the right.

3 How to identify the essence: the concept of attributes

If the right to the protection of personal data were an absolute right, its entire definition would correspond to the essence, a point also made by Brkan.[25] However, Article 8 of the

[24] This is possibly akin to the ancillary or instrumental approach to data protection proposed by Raphaël Gellert and Serge Gutwirth, "The legal construction of privacy and data protection", Computer Law and security Review, 29(5), 2013.

[25] "In Search of the Concept of Essence of Eu Fundamental Rights through the Prism of Data Privacy."

Charter is a qualified right; [26] in this case, talking about the essence, or core areas, of a right begs the question as to what constitutes the peripheries of a right – i.e. tracing its boundaries. After surveying the literature addressing boundaries of the right to the protection of personal data, I propose a method to identify such boundaries.

3.1 LITERATURE ON BOUNDARIES AND THE ESSENCE

To begin with, it should be recalled that the discussion on 'boundaries' is as old as the question of the independence of 'data protection' from 'privacy', a question kept alive by the inconsistent approach of the Court to Article 8.[27] However, the discussion on boundaries strongly overlaps with that of fair information principles or FIPs[28] through which data protection was first proposed, as well as the search for principles of privacy, a search which abounds in the literature (akin to most rights which, as De Hert rightly notes, lend themselves to being articulated in terms of principles[29]).

For the sake of this discussion, which concerns the jurisdiction of the EU, I limit myself to attempts made by recent scholarship to identify the boundaries of the right as enshrined in the Charter. A number of attempts, despite their elegance and subsequent success, conflate Art. 7 of the Charter with Art. 8 under the common umbrella of 'privacy'. This is the case of Finn, Wright, and Friedewald's[30] understanding of the right. The typology proposed by Koops, Clayton Newell, Timan, Skorvanek, Chokrevski and Galic[31] similarly addresses 'privacy', and transcends the boundaries of the EU: the Charter is taken into account, but only as one piece of the regulatory jigsaw puzzle creating regulatory convergence across the two sides of the Atlantic. Nevertheless, the question of regulatory convergence is relevant and acquires particular weight in relation to datafication and the design of technology, issues which, pursuant to the new rules in the General Data Protection Regulation (hereafter GDPR),[32] should no longer be an afterthought. I will come back to this point in the conclusions.

Attempts to identify, directly or indirectly, the boundaries and essence of the right to the protection of personal data have been made, in chronological order, by De Hert, Tzanou,

---

[26] Similarly to the right to respect for private and family life, personal data protection is not absolute, but must be considered in relation to its function in society. Judgment of 17 October 2013 in Schwarz, C-291/12, EU:C:2013:670, para 33 (2013); *Judgment of 5 May 2011 in Deutsche Telekom, C-543/09, ECLI:EU:C:2011:279*, para 51 (2011).

[27] This is discussed at length and convincingly in Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right in Europe* (Springer, 2014); Orla Lynskey, *The Foundations of Eu Data Protection Law* (Oxford: Oxford University Press, 2015). Tzanou refers to the Court's incoherent approach as the "data protection paradox", which stands in the way of the autonomous character of personal data protection. Tzanou (2012), p. 353.

[28] Alan Westin, *Privacy and Freedom* (Atheneum Press, 1967); Robert Gellman, "Fair Information Practices: A Basic History (Version 1.89)," Constantly updated at: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[29] Paul De Hert, "Data Protection as Bundles of Principles, General Rights, Concrete Substantive Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (Foreword)," *European Data Protection Law*, no. 2 (2017): p. 167.

[30] Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Ronald Leenes Serge Gutwirth, Paul de Hert, and Yves Poullet, (Dordrecht: Springer, 2013).

[31] Bert-Jaap Koops et al., "A Typology of Privacy," *University of Pennsylvania Journal of International Law* 38 (2017).

[32] *Regulation 2016/679/Eu of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/Ec (General Data Protection Regulation), Oj L 119/1*.

Gellert and Gutwirth,[33] Bygrave, Lynskey[34] and Brkan. In the context of the discussion of privacy impact assessments (IA), De Hert[35] appraises the possibility of building a data protection IA, which indirectly entails defining the boundaries of data protection. He argues that the nature of the right to data protection hinders the conclusion of a real IA; the right's nature calls instead for a compliance check based on the requirements laid down in legislation. He then lists some of the classic principles or FIPs, namely: legitimacy, purpose restriction, security and confidentiality, transparency, data subject's participation and accountability. He does not propose a method to define them, however, or advance a possible notion of the essence. In a more recent piece, De Hert proposes to look at data protection as a bundle of (general and concrete subjective) rights, principles and rules representing a small part of EU administrative law. Adapting a quote from literary author Haruki Murakami, he claims that data protection is inherently hollow: "Data protection has no vision of the future. It is loosely organized around unfixed principles but has no desire to realize them".[36]

Conversely, Tzanou originally hinted at a possible method to identify core areas of Art. 8 based on positive law, which, however, she abandoned in later stages of her research.[37] In her latest book, she claims that the meaning of Art. 8 should be independent from secondary law and be linked instead with the overarching values that the right pursues: privacy; transparency, accountability and due process; non-discrimination; proportionality; and dignity. She rightly acknowledges that Art. 8 incorporates a subset of FIPs, each of which could subsume further FIPs, and also notes that FIPs other than those contained in the definition of Art. 8 may express the essence of the right.[38]

Gellert and Gutwirth [39] also challenge the idea that we could ever reach the essence of the right to the protection of personal data (and private life). Their approach, which potentially challenges this research, is addressed in the conclusions.

Bygrave[40] discusses the boundaries of 'data privacy', that is the protection of personal data, decoupled from considerations of private life. He identifies seven tenets: i) fair and lawful processing; ii) proportionality; iii) minimality; iv) purpose limitation; v) data subject influence; vi) data quality; and vii) sensitivity. He advances the idea that opposition to automated decisions may be a nascent principle, but he does not articulate this idea further. Besides the fact that, as I will argue, 'sensitivity' cannot be considered a tenet in EU law, his typology is, similarly to Koops et al, also construed in the interest of regulatory convergence.

Lynskey notes that the concept of the essence "remains elusive"[41] because of the abovementioned confusion of the Court with regards to Art. 8, as well as the lack of consensus concerning which data protection rules are more fundamental.[42] This problem comes partially from the fact that data protection remains intrinsically connected to privacy, a point which I

[33] Serge Gutwirth and Raphael Gellert, "The Legal Construction of Privacy and Data Protection," *Computer Law & Security Review* 29 (2013).
[34] Lynskey, *The Foundations of Eu Data Protection Law*.
[35] Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments," in *Privacy Impact Assessment*, ed. Paul De Hert and David Wright, Law, Governance and Technologies Series (Dordrecth and New York: Springer, 2012).
[36] "Data Protection as Bundles of Principles, General Rights, Concrete Substantive Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (Foreword)," p. 179.
[37] Maria Tzanou, "Eu Counter-Terrorism Measures and the Question of Fundamental Rights: The Case of Personal Data Protection" (PhD thesis, European University Institute, 2012).
[38] Maria Tzanou, The fundamental Right to Data Protection, Normative Value in the Context of Counter-terrorism surveillance (Oxford and Portland: Hart 2017).
[39] Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative," *International Data Privacy Law* 5, no. 1 (2015).
[40] Bygrave, *Data Privacy Law*.
[41] Lynskey, *The Foundations of Eu Data Protection Law*, p. 271.
[42] Ibid., pp. 270-72.

share and elaborate elsewhere.[43] According to Lynskey, the suggestion by the AG contained in the Opinion on *Rijkeboer*, whereby all elements of secondary law which are found in the definition of Art. 8 could be seen as 'essential components' of the right, is a possible method to find the essence, though this is not explored in practice.[44] Moreover, she equates essential components with the essence, despite the fact that, as mentioned at the beginning of this section, data protection is a qualified right. When commenting *Digital Rights Ireland*, which risks embodying the logical fallacy – also observed by Purtova[45] - of distilling the core of a right from secondary law, Lynskey hints at the possibility that the Court claimed data security to be the essence of Art. 8 from the perspective of a holistic reading of the right. She suggests that the essence of data protection could actually be privacy, whilst other 'essential components' of the right would play a peripheral role (but does not define them further). In other words, not all elements of secondary law found in the definition of the right would have a fundamental character.

Finally, Brkan proposes a methodology,[46] based on the exclusionary approach to the essence, which is contextual to a case and does not lead to an identification of clear boundaries.

3.2 A METHODOLOGY TO IDENTIFY THE ATTRIBUTES AND ESSENCE OF ART. 8

None of the works surveyed above proposed a working method to define the boundaries of Art. 8 of the Charter, and most of them challenge the feasibility of finding its essence. Yet, ascertaining the scope of the essence is of crucial practical application, for instance when developing new technology, assessing its possible use and choosing between policy alternatives.[47] The approach proposed here starts from an identification of the boundaries of the right, using the concept of 'attributes' as the intrinsic and distinctive substantive dimensions of a right. I borrow this concept from the work of the OHCHR[48] (supported by the Fundamental Rights Agency[49]), and the UK Equality and Human Rights Commission,[50] where it was developed in the context of indicators.

---

[43] The two rights meet at the intersection of identity (and related personality), autonomy and dignity and act in synergy, as I argue in Maria Grazia Porcedda, "The Recrudescence of 'Security V. Privacy' after the 2015 Terrorist Attacks, and the Value of 'Privacy Rights' in the European Union," in *Rethinking Surveillance and Control. Beyond the "Security Versus Privacy" Debate*, ed. Elisa Orrù, Maria Grazia Porcedda, and Sebastian Volkmann-Weydner (Nomos, 2017), p. 164. See also Maria Tzanou, The Fundamental Right to Data Protection, Normative Value in the Context of Counter-terrorism surveillance (Oxford and Portland: Hart 2017).

[44] Lynskey, *The Foundations of Eu Data Protection Law*, pp. 267-68.

[45] Nadezhda Purtova, "Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination Off the Table... And Back on Again?," *Computer Law & Security Review* 30, no. 1 (2014). Quoted in Lynskey, *The Foundations of Eu Data Protection Law*.

[46] Brkan, "In Search of the Concept of Essence of Eu Fundamental Rights through the Prism of Data Privacy," pp. 24-26; "The Concept of Essence of Fundamental Rights in the Eu Legal Order."

[47] This was proposed and developed in the context of the SurPRISE and SURVEILLE FP7 projects. I discuss the use of the essence in relation to the fight against cybercrime and the pursuit of cyber security in Maria Grazia Porcedda, "Cybersecurity and Privacy Rights in Eu Law. Moving Beyond the Trade-Off Model to Appraise the Role of Technology" (PhD Thesis, European University Institute, 2017)

[48] United Nations, "Report on Indicators for Monitoring Compliance with International Human Rights Instruments," p. 3.

[49] Fundamental Rights Agency, "Using Indicators to Measure Fundamental Rights in the Eu: Challenges and Solutions," in *2nd Annual FRA Symposium Report* (Vienna2001).

[50] Jean Candler et al., "Human Rights Measurement Framework: Prototype Panels, Indicator Set and Evidence Base," (London: Equality and Human Rights Commission, 2011). I used this to develop the attributes of article 7 of the Charter in Maria Grazia Porcedda, "Cybersecurity and Privacy Rights in Eu Law. Moving Beyond the

Attributes are "a limited number of characteristics of [a given] right." (…). To the extent feasible, the attributes should be based on an exhaustive reading of the standard, starting with the provisions in the core international human rights treaties; (…) the attributes of the human right should collectively reflect the essence of its normative content (...). To the extent feasible, the attributes' scope should not overlap."[51] Attributes represent the synthesis of what would otherwise be the 'narrative' on legal standards of a human right. In the context of the OHCHR work, attributes are the first step to build structural indicators, one of three[52] sub-indicators which measure the commitment of a state towards certain human rights objectives.

In the context of this enquiry, attributes can be used as a powerful instrument to capture the granularity of the intrusiveness into fundamental rights, in that they can help identify core areas of rights, the limitation of which would be impermissible. In this sense, the identification of attributes is a preliminary step toward the identification of essence/core(s), and therefore comes logically before them. The relationship between attributes and essence can be articulated in two ways. On the one hand, the essence can be seen as the core of an attribute. This option seems in line with the Court's case law on the essence of Art. 8 reviewed earlier. On the other hand, some attributes may be seen as peripheral, while other attributes could coincide or express a core area. This second option seems to have some traction in the literature, but could lead to conflicts in the application of the law, given the qualified nature of the right to the protection of personal data. Here I follow the first approach and, in line with current case law, submit that there may be multiple essence, or core areas.

To identify the attributes of the right to the protection of personal data, I rely, by analogy, on the method developed by the OHCHR, and focus on its first step,[53] which consists in discerning the applicable legal framework, which includes all applicable instruments, including international ones, case law and authoritative interpretations. Attributes are derived from such a framework; they should be as few as possible, mutually exclusive and able to capture the full meaning of the right. While this exercise is experimental, because the OHCHR methodology requires validation of the attributes by a group of experts, at the same time it benefits from the well-established discussion of (fair information) principles of personal data. Indeed, as noted earlier, the right itself evolved from a series of principles, and the wording of Art. 8 of the Charter, which incorporates some (but not all) of the classic principles, testifies to this. The attributes will thus result from a mix of principles, relevant case law and authoritative interpretations.

The OHCHR does not address the notion of the essence (unless we follow the approach whereby some attributes coincide with core areas of the right). As seen, the CJEU has identified two substantive notions of the essence of the right, which must be expressed in a rule, without however explaining the rationale of its choice. Moreover, in at least one case, the Court has adopted a procedural approach to the essence. I suggest supplementing the findings of the Court with a purposive interpretation of the right, whereby the essence should express the elements that aim to fulfil the goal(s) or values of the right.

Trade-Off Model to Appraise the Role of Technology" (PhD Thesis, European University Institute, 2017); "Privacy by Design in Eu Law. Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection ", Annual Privacy Forum 2018, Lecture Notes in Computer Science, forthcoming.

[51] United Nations, High Commissioner for Human Rights (OHCHR), "Human Rights Indicators. A Guide to Measurement and Implementation," in *HR/PUB/12/5* (New York and Geneva2012), p. 31.

[52] The other two sub-indicators correspond to the criteria of process and outcome.

[53] United Nations, "Report on Indicators for Monitoring Compliance with International Human Rights Instruments," p. 3. The second and third steps consist in reviewing the attributes, and validating them respectively.

4 Applying the OHCHR method to the right to the protection of personal data

4.1 STEP ONE: THE APPLICABLE LEGAL FRAMEWORK

This enquiry concerns Article 8 of the Charter of Fundamental Rights: the identification of the attributes and essence of this right is based on the specific hierarchy of norms of EU law,[54] and hence there is no pretence of universal application here.

Attributes should be first distilled from Article 8 of the Charter, Article 39 TEU and Article 16 TFEU, as interpreted by the judgments of the CJEU (ECJ and General Court) *after the Charter acquired primacy* with the entry into force of the Lisbon Treaty (hence since December 2009).[55] Unlike most judgements which see Art. 8 as being joined at the hip with Art. 7, I propose that the right to the protection of personal data be interpreted in light of article 52(2) of the Charter, whereby "rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties". There are two intertwined reasons justifying this choice. First, Art. 8 is not among the rights deriving from the ECHR listed in Art. 52(3), a view AG Saugmandsgaard Øe recently corroborated in an *obiter dictum* to his Opinion on *Tele2Sverige*[56] (though the point was, unfortunately, not taken up in the judgment). Secondly, and in further development to suggestions made by González Fuster,[57] it was first introduced as a right in EU law through Art. 286 of the Treaty of Amsterdam.

Reading a right in the light of Art. 52(2) of the Charter means, as argued by Craig,[58] that the CJEU should take into sufficient account secondary law, whenever this has extensively refined the purview of a right whose legal basis is found in the Treaty. This could be supported by what the Court said, among others, in *Google Spain and Google*, whereby the requirements of Article 8(2) and 8(3) of the Charter "are implemented *inter alia* by Articles 6, 7, 12, 14 and 28 of Directive 95/46."[59]

As a result, the regime contained in rules for the processing of personal data adopted pursuant to Article 16 TFEU and 39 TEU represents a correct implementation of the right, at least until the Court rules the opposite, as it stated in *Schrems.*[60]. Hence, such rules should also

---

[54] Allan Rosas and Lorna Armati, *Eu Constitutional Law - an Introduction* (Oxford and Portland, Oregon: Hart Publishing, 2010).

[55] Such limitation is justified by the fact that, until the Charter acquired primacy, the Court did not analyse cases concerning the protection of personal data under the light of Article 8 of the Charter, limiting itself to references in passing.

[56] "Article 8 of the Charter, which was interpreted by the Court in Digital Rights Ireland, establishes a right that does not correspond to any right guaranteed by the ECHR, namely the right to the protection of personal data, as is confirmed, moreover, by the explanations relating to Article 52 of the Charter. Thus, the rule of interpretation laid down in the first sentence of Article 52(3) of the Charter does not, in any event, apply to the interpretation of Article 8 of the Charter." Opinion of AG Saugmandsgaard Øe of 19 July 2016 in Tele2 Sverige and Watson and others, Joined cases C-203/15 and C-698/15, EU:C:2016:572, Paragraph 79 (2016).

[57] For a more extensive articulation of this approach, and its implications, please refer to Porcedda, "Cybersecurity and Privacy Rights in Eu Law," chapter 7. See also González Fuster, *The Emergence of Personal Data Protection*.

[58] Otherwise Article 52.2 would be in tension with the idea that the provisions of the Charter enjoy the same legal status as the Treaties, as constitutional provisions could be limited by secondary legislation, whenever the Treaty provisions are formulated in generic terms; it would also conflict with the idea that fundamental rights are used as instruments to challenge the validity of EU law. Craig, *The Lisbon Treaty*.

[59] *Judgment of 13 May 2014 in Google Spain and Google, C-131/12, Ecli:Eu:C:2014:317*, paragraph 69 (2014).

[60] In an *obiter dictum*, para 52, the Court said "Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn".

be taken into account when defining the regime for permissible limitations, to which, as stated above, the right to the protection of personal data is subject (construed -narrowly like all exceptions[61]- in the light of the Treaty and the Charter, and general principles of EU law).

This approach bears an important consequence for the role of Art. 8 ECHR[62] *vis-à-vis* Art. 8 of the Charter. In accordance with settled jurisprudence of the CJEU, the case law of the ECtHR holds 'special significance'[63] in the interpretation of the scope and meaning of the right to the protection of personal data (whenever it touches upon the matter), but the latter is not strictly constrained by it. The rationale is to ensure the independence of Union law and its capability of offering greater protection than interpretations pursuant to Article 8 ECHR (which, it should be recalled, represent minimum safeguards that EU law is encouraged to surpass[64]).

Of greater importance in defining the content of the attributes is Convention 108[65] (and its related case law, with the caveats discussed above), an instrument of international law, which has a bearing on the interpretation of EU law. [66] This is for several reasons. First of all, Convention 108 introduced the concept of the protection of personal data as a right. Secondly, it offered the blueprint for the drafting of Directive 95/46, particularly in the part that concerns FIPs (which were, in turn, developed in dialogue with the OECD Guidelines[67]). By extension, any discussion on the attributes of the protection of personal data cannot ignore the FIPs. Finally, because the instrument, and especially the Modernised Convention 108, will provide insight into what represents a minimum threshold of the right. Following Recital 105 of the GDPR, adoption of the Convention by a third country is a crucial criterion to decide the adequacy of the legislation of such third country with a view to allow data transfers.

4.2 STEP TWO: IDENTIFICATION OF THE ATTRIBUTES

The purpose of this section is to identify attributes of the right to the protection of personal data, and to propose potential core areas, or the essence, relating to such attributes.

The CJEU last reaffirmed in *Schrems* that the control performed by an independent authority is an 'essential component' of the right, because it is listed in the definition of the

---

[61] In the context of Article 8, see, for instance, Judgment of 11 December 2014 in Ryneš, C-212/13, EU:C:2014:2428, para 29 (2014). Moreover, to ensure that the objective set in secondary law is attained, its provisions § 53 "cannot be interpreted restrictively", and they have "broad territorial scope". *Google Spain and Google*, paras 53-54.

[62] *Convention for the Protection of Human Rights and Fundamental Freedoms (as Amended by Protocols No 11 and 14), Council of Europe, Ets N° 005, 4 November 1950*, (4 November 1950).

[63] Opinion of the Court of 18 December 2014, Avis 2/13, EU:C:2014:2454, paragraph 37 (2014).

[64] A second, more far-reaching consequence, is that the case law of the ECtHR should not supersede Union law in case of conflict of interpretation, which has a strong bearing on the scope of the right and hence on permissible limitations. In practice, this may mean that Article 8 ECHR would have a different relevance depending on the difference in scope of private life and data protection, e.g. as described by Kranenborg. Herke Kranenborg, "Access to Documents and Data Protection in European Union: On the Public Nature of Personal Data," *Common Market Law Review* 45 (2008): p. 1094. For a complete elaboration of this view, see Porcedda, "Cybersecurity and Privacy Rights in Eu Law", chapter 7.

[65] ; Council of Europe, "Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data," (2016); Amending protocol to the Convention for the Protection of
Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

[66] E.g. Judgment of 16 October 2012 in Hungary v. Slovakia, C-364/10, ECLI:EU:C:2012:630, para 44. This varies on the basis as to whether the EU is a party to the instrument, or not.

[67] *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Organization for the Economic Cooperation and Development, C(80)58/Final, as Amended on 11 July 2013 by C(2013)79*, (11 July 2013).

right (§ 40-41). As expounded in section 2, the 'essential component' is unlikely to constitute the essence; nevertheless, I submit that 'essential component' can correspond to the notion of attributes. By analogy, all elements contained in the definition of Art. 8 should be considered an essential component of the right. If we discount the coincidence between attributes and essence (due to the fact that Art. 8 is a qualified right), this is similar to Lynskey's argument based on the AG's Opinion in Rijkeboer: all elements contained in the applicable law which are found in the definition of the right should be seen as essential components of the right. As mentioned earlier, in *Google Spain and Google* the Court declared that the requirements of Article 8(2) and 8(3) of the Charter "are implemented *inter alia* by Articles 6, 7, 12, 14 and 28 of Directive 95/46", which specify further principles; the same must apply to the GDPR. Moreover, in *Digital Rights Ireland* and *Opinion 1/15* the CJEU identified the essence of the right from requirements which are not, strictly speaking, part of the definition (though see section 5.4), but instead are clearly stated in secondary law and the old Convention 108. Hence, and *a fortiori*, it should be possible to identify elements of secondary law that, due to their importance (as testified by their inclusion in the Modernised Convention 108, Opinions or backing by the literature), can be seen as attributes of the right.

As mentioned above, any discussion on the attributes of the protection of personal data must engage with the FIPs. Yet, here it is apt to recall that attributes should be as few as possible, mutually exclusive, and capable of capturing the full meaning of the right. Moreover, the definition of the right does not embrace all principles of the GDPR, which in turn do not coincide with FIPs, as also noted by De Hert.[68] As a result, not all existing principles must necessarily be translated into independent attributes. Moreover, some principles/FIPs representing the duty of a controller are implied in a facet of the right. For instance, the principle of accountability is not contained in Art. 8, but is implied by the right to oversight expressed in Art. 8(3). Similarly, the principle/FIP of accuracy is implied by the right to rectification.

Table 1 illustrates the mismatch between FIPs, principles in the GDPR, and those found in the definition of the right. The top row contains the principles, and the acronym 'FIP' in brackets indicates that the corresponding principle is also a fair information principle (accompanied by the original name when relevant). The left column refers to Article 8 and the GDPR. The presence of the principle in the relevant legal instrument is signalled with the dummy variable "X" or the corresponding Article (no value means absence).

Principles / Instrument	Fairness	Lawfulness/consent	Purpose limitation (FIP)	Use limitation (FIP)	Collection limitation (FIP)	Transparency (FIP openness)	Individual rights (FIP participation)	Accuracy (FIP data quality)	Accountability (FIP)	Independent control	Integrity and confidentiality (FIP security)
Art. 8	X	X	X			X if with fairness	X	X		X	Notion of protection ?

[68] De Hert, "Data Protection as Bundles of Principles, General Rights, Concrete Substantive Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (Foreword)."

GDPR	Art. 5.1(a.)	Aart. 5.1(a.)	Art. 5.1(b) and (e)	Art. 5.1(b)	Art. 5.1 (c)	Art. 5.1(a)	Chapter III	Art. 5.1(d)	Art. 5.2	Chapter VI	Art. 5.1(f)

Table 1 Comparison of data protection principles: FIPs, GDPR and Article 8 of the Charter

4.3 STEP THREE: RELEVANT LITERATURE

In line with calls from the OHCHR method to supplement the applicable law with what it calls 'authoritative' literature, the identification of the attributes benefits from the elaboration of data protection principles proposed by the literature covered in section 3.1. The work of Bygrave[69] is relevant because, first, he suggests that opposition to automated decisions could be a nascent principle of data protection, and second, he rightly argues that one of the sources of data protection is to be found in the rule of law. Such a source is visible in the formulation of FIPs and the ensuing first limb of Article 8.2 of the Charter: "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."*

The argument advanced by De Hert[70] in relation to data protection impact assessments lends a hand in developing the reasoning concerning attributes that derive from the rule of law, namely fairness, purpose limitation and lawfulness, as well as independent oversight. These are likely to be more easily subjected to a compliance check, rather than an evaluation of their substance; in this respect, those attributes are possible candidates for the essence understood in procedural terms.

Tzanou's and Lynskey's work are of relevance for identifying the essence, to which I move next.

4.4 STEP FOUR: IDENTIFICATION OF THE ESSENCE

As seen, the CJEU has identified two notions of the essence of the right; the existence, in a given legal instrument, of rules protecting the integrity, confidentiality and security of the data, as well as rules on purpose limitation. The Court's choice implies that there can be more than one essence, and that such essence should be expressed in a rule. The Court did not, however, explain the reasoning of its choice. I suggest supplementing the findings of the Court with a purposive interpretation of the right, whereby the essence should express the elements of the attribute that aim to fulfil the goal(s) or values of the right. Such an idea is rooted in the law and society approach to rights argued, for instance, by Bobbio and Pugliese.[71]

As noted earlier, Tzanou's proposition that the essence should reflect the ultimate goals of the right also supports a purposive understanding of the essence, though I disagree with her idea that the essence should not be substantively determined. Similarly, Lynskey's suggestion that the choice of the Court to equate data security with the essence follows a 'holisitic' approach to Art. 8, could possibly go in the direction of a purposive understanding of the right. I disagree with Lynskey's proposal that the essence of data protection could be privacy. By contrast, I suggest both rights help the individual keep (solid) control of the process overseeing

[69] Bygrave, *Data Privacy Law*.
[70] De Hert, "A Human Rights Perspective on Privacy."
[71] Norberto Bobbio, *L'età Dei Diritti* (Torino: Einaudi, 1997); Giovanni Pugliese, "Appunti Per Una Storia Della Protezione Dei Diritti Umani," *Rivista trimestrale di diritto e procedura civile* 43, no. 2 (1989); Porcedda, "The Recrudescence of 'Security V Privacy' after the 2015 Terrorist Attacks," p. 149.

the creation and maintenance of her or his identity and, relatedly, dignity and autonomy, but each does so in a different manner and expresses different core areas.[72]

The right to the protection of personal data provides reassurance that, once a person has expressed her or his (necessarily complex) identity, the integrity of such identity will receive protection. At a deeper level, such protection acts as a filter against direct or indirect attempts to deny the richness of one's personality, allowing the person to evolve and change, that is, to exercise her autonomy. At a more superficial level, such protection tries to pre-empt, or at least minimize, the harms that can ensue from the flattening of one's personality against categories, determined by bureaucratic and economic entities, to (legitimately) provide or deny access to goods and services.[73] The essence should act as the bulwark against the assault on these values.

5 The attributes and the essence of Art. 8

The table below summarizes the attributes discussed here. Attributes I to III derive from the formulation of Article 8. Attributes IV and V do not derive directly from Art. 8 but have strong backing in legal instruments, case law and the literature. In the following, each section is devoted to a single attribute. I first introduce the attribute, then I discuss the applicable law supporting it and further specifying it, and then I propose the essence; a partial exception is represented by the last attribute, where I follow the opposite route because of the case law of the CJEU. Note that the attributes were identified on the basis of the GDPR only. Further research may include an analysis of the Police Directive and the implementation by its Member States.

Attributes from Article 8	Essence unambiguously identified by the Court	Attributes found in secondary law and Convention 108 /literature
I. Legitimate processing (rule of law) • Fairness/transparency • Purpose limitation • Lawfulness	Purpose limitation	
Oversight (partly rule of law) **II. Independent oversight**		Oversight (partly rule of law) **IV. Human intervention (automated decisions)**
III. Data subject's rights • Access • Rectification & accuracy	Data security	**V Data security and minimization**

[72] For a further elaboration of this argument, and the literature on which it is based, please refer to "The Recrudescence of 'Security V Privacy' after the 2015 Terrorist Attacks," pp. 164-67. For a quick overview of the essence of Art. 7, see "Privacy by Design in Eu Law. Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection ".

[73] As explained in greater detail, and with the support of rich literature, in "The Recrudescence of 'Security V Privacy' after the 2015 Terrorist Attacks."

• Objection, including profiling • Erasure (right to be forgotten) • Portability • Restriction

Table 2 List and sources of attributes, and the essence found by the Court

5.1 LEGITIMATE PROCESSING (ATTRIBUTE OF THE RULE OF LAW I)

This attribute stems from the first limb of Article 8(2) of the Charter: "Such data must be processed fairly for specified purposes on the basis of the consent of the person concerned or some other legitimate basis laid down by law". It refers to the expectation of the data subject that the processing must be legitimate, in all three senses expounded in the Article: in relation to data protection law as a whole (fairness), the interests of the controller in pursuing the processing (purpose specification/limitation), and the legal system/*ordre public* as a whole (lawfulness).

The three principles pave the way to a single attribute because they are not mutually exclusive, but rather cumulative. This is due to their common roots in the rule of law, which effects functional interconnections. To be sure, the three principles only represent some of the tenets of the rule of law as understood in the EU.[74] In detail, fairness stems from legal certainty (and lawfulness), purpose specification from proportionality and non-arbitrariness, and lawful processing from legality. Hence the attribute is called 'legitimate processing'.

Secondary law and interpretations thereof support such interconnections. First, Article 5(1) (a) of the GDPR states that personal data must be "processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)". Article 6 of the GDPR on conditions of lawfulness, and particularly its paragraph 3, clearly refers to purpose specification and fairness.[75] Likewise, the conditions whereby processing operations other than those for which the personal data have been collected are compatible with the original purpose, specified

[74] These are: legality, legal certainty; prohibition of arbitrariness of the executive powers; independent and impartial courts; fundamental rights; and equality before the law. European Commission, "A New Eu Framework to Strengthen the Rule of Law," in *(Communication) COM (2014) 158 final* (2014). These reflect the constitutional traditions of the Member States and widely correspond to the tenets developed by the Council of Europe's Venice Commission taking into account ECtHR Law. Council of Europe, European Commission for Democracy through Law (Venice Commission), "Report on the Rule of Law," in *Study No. 512/2009* (2011).

[75] In connection to the legitimate aim of the controller, see *Judgment of 13 May 2014 in Google Spain and Google, C-131/12, Ecli:Eu:C:2014:317*, § 74; Judgment of 30 May 2013 in Worten, C-342/12, ECLI:EU:C:2013:355, § 45 (2013). In the former, the Court stated "the processing…can be considered legitimate…under the legitimate interests of the controller, but that ground…necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Article 7 and 8 of the Charter." In the latter, the court ruled that "national legislation---which requires an employer to make the record of working time available to the national authority responsible for monitoring working conditions" is not precluded.

in Article 6(4) of the GDPR, [76] read together with Recital 50,[77] clearly connect with specification, fairness and consent.

With regards to purpose specification/limitation, the Article 29 Data Protection Working Party noted that it is "preliminary to several other data protection tenets and contributes to "transparency, legal certainty and predictability", which in turn enable control by the data subject".[78] Furthermore, the Working Party submits that the purpose must be legitimate, specific and explicit to both controller and data subjects, thus encapsulating fairness.[79] As the Court declared in *Digital Rights Ireland*, using data for several purposes without the data subject "being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[80]

The provisions on consent, [81] as defined in Article 4(11) of the GDPR,[82] read in the light of Recital 32,[83] also link to fairness and purpose limitation. Consent has to be assessed in the light of the whole Regulation, in that, pursuant to Article 7(2) of the GDPR, "consent given in the context of a written declaration…which constitutes an infringement of this Regulation shall not be binding".[84]

On the basis of the applicable law just expounded, the functional interconnection of the three principles can be easily explained. If a processing is not fair, then there is no guarantee of purpose limitation, which would void consent or challenge lawfulness. If the purposes of the processing are indeterminate, then the processing cannot be fair, paving the way to uninformed consent and a general disrespect of lawfulness. If the processing is carried out without consent or pursuant to the wrong legal basis, then it is unfair, and there is no guarantee that the purpose is specified and limited as expected.

---

[76] The Article follows the recommendations issued by the Article 29 Data Protection Working Party. Accordingly, the legislator prohibits incompatibility; hence, a different purpose may not necessarily be incompatible, and the assessment must be substantive and on a case-by case basis. Article 29 Data Protection Working Party, "Opinion 03/2013 on Purpose Limitation," in *00569/13/EN WP 203* (2013). See also *ASNEF* and *FECEDM*, where the Court ruled that further processing of personal data in the absence of consent cannot be limited to data that are already available in the public domain. Judgment of 24 November 2011 in ASNEF and FECEDM, joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777 (2011).

[77] Whereby further processing operations "should be allowed only where the processing is *compatible* with the purposes for which the personal data were initially collected." Moreover, in order to ascertain the compatibility of a further processing with the original purpose, the controller must first meet "all the requirements for the *lawfulness* of the original processing" and should take into account "any link between those purposes and the purposes of the intended further processing" and "the context in which the personal data have been collected, in particular the *reasonable expectations* of data subjects based on their relationship with the controller as to their further use". Hence, "the passing of the same data to another undertaking intending to publish a public directory without renewed consent having been obtained from the subscriber is not capable of substantively impairing the right to the protection of personal data, as recognized in Article 8 of the Charter." *Judgment of 5 May 2011 in Deutsche Telekom, C-543/09, Ecli:Eu:C:2011:279*, § 66.

[78] "Opinion 03/2013, Wp 203," p. 11.

[79] Hence, a purpose that is vague or general, such as 'improving users' experience', or 'marketing purposes' will not fulfil the requirement of specificity.

[80] *Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, Ecli:Eu:C:2014:238*, § 37 (2014).

[81] The court ruled that denial of consent to transfer (process) one's data can only be overruled if the potential controller establishes the necessity of such processing (in relation to one of the grounds for lawful processing). *Judgment of 29 June 2010 in Bavarian Lager Ltd., C-28/08 P, Ecli:Eu:C:2010:378*, § 77 (2010).

[82] Which reads "any freely given, *specific*, *informed* and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

[83] "…Consent should cover all processing activities carried out for the *same purpose* or purposes. When the processing has *multiple purposes*, consent should be given for all of them."

[84] Moreover, "where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data" (Article 7(1) of the GDPR).

Perhaps the case lending the strongest support to this attribute is *Digital Rights Ireland*,[85] where the Court ruled, in relation to the Data Retention Directive[86] (focussing on storage limitation), that "the EU legislation in question must lay down clear and precise rules …so that the [concerned] persons …have sufficient guarantees to effectively protect their personal data against the risk of abuse…".[87]

***

In *Opinion 1/15,* the CJEU clarified that rules on purpose limitation constitute the essence of Art. 8. This fulfils the expectation that the data subject's data will not be used to characterize him or her out of context, and create an impact over which he or she has no control.

5.2 TWO ATTRIBUTES EXPRESSING OVERSIGHT

Oversight refers to the availability of some form of control to ensure the respect of the principles relating to the processing of personal data and is the counterpart to the pricinple of accountability of the data controller. Oversight is embodied in two attributes.

5.2.1Independent supervisory authority (Attribute of the Rule of Law II)

The first attribute is distilled from Article 8(3) and refers to the availability of an independent public authority monitoring compliance with data protection laws. The existence of a supervisory authority, which is conceived as the guardian of the right,[88] is "an essential component of the protection of individuals with regard to the processing of personal data"[89] because it is enshrined in "primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU".[90]

Like the previous attribute, it has a strong basis in the rule of law, particularly in the availability of independent courts and an effective remedy. Such overlap, also noted by De Hert,[91] should not be seen as implying the redundancy of personal data protection, but, as discussed earlier in section 2, rather as a demonstration of the interdependency and interrelatedness of fundamental rights.

According to Article 4(21) of the GDPR, a supervisory authority is an independent public authority that is established by a Member State. Whereas Member States are free to choose the most appropriate institutional model for the authority,[92] such a model must ensure

[85] *Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238*, paragraph 54.

[86] *Directive 2006/24/Ec of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/Ec, Oj L 105/54 (Data Retention Directive)*, OJ L 105/54, (13 April 2006).

[87] Moreover, under certain conditions, "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed." *Judgment of 13 May 2014 in Google Spain and Google, C-131/12, Ecli:Eu:C:2014:317*, § 93.

[88] *Judgment of 16 October 2012 in Commission V. Austria, C-614/10, Ecli:Eu:C:2012:631*, § 52 (2012). The Court refers here to the 'right to privacy'.

[89] *Judgment of 6 October 2015 in Schrems, C-362/14, Ecli:Eu:C:2015:650*, § 41.

[90] Ibid., § 40.

[91] De Hert, "Data Protection as Bundles of Principles, General Rights, Concrete Substantive Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (Foreword)."

[92] *Judgment of 8 April 2014 in Commission V. Hungary, C-288/12, Ecli:Eu:C:2014:237*, § 68 (2014).

"independence". [93] The essential criteria for independence are found in Articles 51 and 52 of the GDPR, which codified the findings of case law,[94] and are the absence of directions and instructions, as well as of political influence (including the threat of early termination), which could lead to "prior compliance" or partiality. Following *Schrems*, independence, which is intended to ensure the "effectiveness and reliability of …the protection of individuals",[95] should be also exercised *vis-à-vis* the Commission.

The provisions on independence serve the ultimate task of supervisory authorities, namely to ensure the appropriate application of data protection rules in order to safeguard data subjects' rights and enable the free flow of personal data.[96] In order to carry out their tasks, authorities are endowed with powers. Those endowed by Directive 95/46 were non-exhaustive;[97] the GDPR codified such findings in Article 58, which harmonizes the powers of supervisory authorities across the Union.

***

The Court has thus far not indicated whether any facet of this limb of the right is to be seen as the essence. A candidate for the essence is therefore the provision, at a minimum, of *ex post facto* supervision.

5.2.2 Human intervention

This attribute concerns the right of a natural person to have another natural person, rather than a machine, take decisions based on the processing of personal data affecting a data subject. Such an individual could be the Data Protection Officer (article 37 of the GDPR) or any data controller.

While this attribute is found primarily in secondary law, particularly in Article 22 of the GDPR, and does not correspond to any existing principles of personal data protection, Article 9 (1) (a) of the Modernized Convention 108 recognizes this entitlement. Moreover, the idea that objection to automated individual decisions could be a nascent attribute/principle of the right was also advanced by Bygrave,[98] who discussed it in the context of the principle 'data subject influence' without developing it further. This attribute and its rationale is intimately linked with the attribute 'data subjects' rights' (also highlighted by Bygrave), particularly the right to object (discussed *infra*). Such recognition is not accidental. This attribute embodies one of the key values of personal data protection advanced in this research: that of retaining control over the portrayal of one's identity (and related personality) to society, and the consequences that can ensue from such portrayal.[99]

---

[93] The ECJ specified that "the words 'with complete independence' in the second subparagraph of Article 28(1) of Directive 95/46 must be given an autonomous interpretation, independent of Article 267 TFEU, based on the actual wording of that provision and on the aims and scheme of Directive 95/46 (see Commission v Germany, paragraphs 17 and 29)." *Judgment of 16 October 2012 in Commission V. Austria, C-614/10, Ecli:Eu:C:2012:631*, § 40.

[94] When the Commission sued Germany, Austria and Hungary for failure to fulfil obligations. *Judgment of 8 April 2014 in Commission V. Hungary, C-288/12, Ecli:Eu:C:2014:237*, § 51-54.

[95] (Paragraph 41), in that a DPA "must be able to examine" the adequacy of a transfer of data (in the context of hearing a claim lodged by a person with reference to such transfer) even if the Commission has already issued a decision pursuant to Article 25(6) of the Data Protection Directive (paragraph 53). To do otherwise would mean depriving individuals of their right to a claim.

[96] Case law suggests that for monitoring to be ensured, the data should be stored in the European Union. *Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined Cases C-293/12 and C-594/12, Ecli:Eu:C:2014:238*, § 68.

[97] Judgment of 1 October 2015 in Weltimmo, C-230/14, ECLI:EU:C:2015:639, § 48-49 (2015).

[98] Bygrave, *Data Privacy Law*, chapter 5.

[99] Which I discuss in Porcedda, "The Recrudescence of 'Security V Privacy' after the 2015 Terrorist Attacks."

The GDPR devotes a number of articles and recitals to the subject matter. Article 22 of the GDPR, which is based on Article 15 of Directive 95/46, reiterates the generic prohibition of taking decisions which produce legal effects or significantly affect a data subject when based solely on automated processing, and a reinforced prohibition against taking such decisions when based on the automated processing of special categories of personal data. Examples of negative effects of such decisions on the data subject include the "automatic refusal of an online credit application or e-recruiting practices without any human intervention" (Recital 71[100]).

Article 22(2), read in the light of Recital 71, provides for exceptions to the general prohibition. When automated decisions are taken pursuant to the exception to this norm, the data subject is entitled to know the logic involved in such automatic processing of data in order to put forward his or her point of view, and appropriate safeguards must be put in place. Indeed, the need to "lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards…. is all the greater where personal data is subjected to automatic processing".[101] In this case, pursuant to Article 22(3) of the GDPR, the controller must provide safeguards consisting *at least* in ensuring "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". The provision of information on such automated processing is mandatory pursuant to Articles 13(2)(f), 14(2)(g) and 15(1)(h), which is consistent with the general obligation of fairness and transparency.[102]

An important innovation of Article 22 of the GDPR, compared with Article 15 of Directive 95/46,[103] is the explicit prohibition of decisions affecting the data subject based solely on profiling, which is defined in Article 4(4) of the GDPR (and recital 71) as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[104] Profiling presupposes monitoring the behaviour of data subjects, which, according to recital 24 of the GDPR, consists in tracking data subjects[105] (on the internet), irrespective of the objective of such tracking. Hence, automated decisions based on profiling are among the processing operations that require conducting an impact assessment (Article 35.3(a); Recital 91). Recital 72 clarifies that profiling "is subject to the rules of this Regulation governing the processing of personal data, and that the future European Data Protection Board should issue suitable guidance".

***

The requirement in the law to obtain, at a minimum, the intervention on the part of the controller has the potential of expressing the essence of this attribute, the infringement of which constitutes a violation of the right. The rationale for limiting automated decisions is that such decisions stem from a partial depiction of the individual, which is based on the expropriation

[100] Moreover, it recommends such decisions not to concern a child (in the GDPR, a child aged 13 or under).

[101] Following the reasoning of *Digital Rights Ireland, Judgment of 6 October 2015 in Schrems, C-362/14, Ecli:Eu:C:2015:650*, § 91.

[102] The controller must inform of "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (see also recital 63 of the GDPR).

[103] The negative change, compared with Directive 95/46, is that Article 22 of the GDPR is subject to the restrictions set by Article 23, as opposed to Article 15 of Directive 95/46, which was not subject to such restrictions. However, Directive 95/46 had limited reach.

[104] See also Article 3(4) of the AFSJ Directive.

[105] The recital refers to the Internet in that it concerns data controllers that are not established in the European Union.

of control over one's identity and the evolution of his or her personality. The proposed essence appears of fundamental importance *vis-à-vis* developments in datafication and the expansion of data science applications (machine learning, data analytics also applied to artificial intelligence, sentiment analysis, etc.), which severely challenge the ability of individuals to control how their data are used to depict themselves, and to take decisions affecting them.

5.3 DATA SUBJECT'S RIGHTS (ATTRIBUTE OF THE RULE OF LAW III)

Data subjects' rights are the last attribute stemming explicitly from the wording of the right in the Charter. The attribute gives substance to the notion of control over one's personal data. Article 8(2) of the Charter mentions the rights of access and rectification. In line with the interpretation given by the Court in *Google Spain and Google,* that the requirements of Article 8(2) of the Charter "are implemented *inter alia* by Articles 6, 7, 12, 14 and 28 of Directive 95/46", the corresponding Articles of the GDPR implement and further specify the content of this attribute. Hence, this attribute means that the individual has, as a general rule, at least six entitlements, subject to the restrictions embodied in Article 23 of the GDPR. The Modernised Convention 108 recognizes most of them, with the exception of the right to portability. Such entitlements vary in the degree of intensity, and relate to each other as preliminary and subsequent steps, or alternative steps, of a strategy geared at controlling one's data and averting the harms that may result from processing operations.

First, pursuant to Art. 8(2) of the Charter, data subjects enjoy the right of access, i.e. to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, to obtain a free copy[106] of personal data being processed (art. 1 GDPR), if possible via electronic means (see also Article 9(1) (b) of Modernised Convention 108).[107] This is particularly the case with health data (recital 63). Such a right to information includes notification of the appropriate safeguards that attach to data transferred outside of the Union. It finds its limits in the potential negative effects it may have on the rights or freedoms of others, including trade secrets or intellectual property, and in particular copyright protecting software (recital 63).

Second, and also pursuant to Art. 8 of the Charter, the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her (Article 16 of the GDPR; Article 9 (1) (e) of Modernised Convention 108). As a result, rectification is instrumental in realizing the principle of accuracy (data quality), whereby the data must be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (Article 5(d) of the GDPR; Article 5(4)(d) of Modernised Convention 108). The importance of rectification and accuracy can be best understood in relation to the 'personal' criterion of data protection, which links it with a person and her or his identity. To maintain accuracy means to respect and reflect the

[106] Hence the interpretation given by the Court in X may be tenable only in part: "In view of the considerations made above in the analysis of Question 2, Article 12(a) of Directive 95/46 must be interpreted as requiring Member States to ensure that the exercise of that right of access takes place without constraint, without excessive delay, and without excessive expense". Judgment of 12 December 2013 in X, C-486/12, ECLI:EU:C:2013:836, § 25 (2013).

[107] This includes, for an applicant for a residence permit, access to all data processed by the national administrative authorities in the guise of a full summary of those data in an intelligible form (allowing that applicant to understand those data and check their accuracy and processing in compliance with that directive), so that the applicant can potentially exercise the other rights conferred by secondary law. Judgment of 17 July 2014 in YS and others, Joined cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081 (2014).

individual's uniqueness, giving relevance to the individual behind the piece of information.[108] Data which are inaccurate become inadequate and hence, in the language of recital 39, "every reasonable step should be taken to ensure" that they are rectified, as seen above, whereas data which are outdated become irrelevant, and hence must be erased. Differently from the Directive, the interpretation given by the Court in *Google Spain and Google*, and the Modernised Convention 108, such a right seems now to limit rectification to the incorrectness of the data, whereas the rectification becomes optional if the stored data "infringes the Regulation or Union or Member State law to which the controller is subject" (recital 65). However, in cases in which the processing is unlawful, then the data subject can claim a stronger entitlement, that of erasure.

This third entitlement of the data subject (the so-called "right to be forgotten" of jurisprudential origins), means that the data subject has a right, under specific conditions, to request and obtain the erasure of personal data concerning him or her without undue delay, particularly when the data subject withdraws consent, the data are no longer necessary, or the processing is or becomes otherwise unlawful (as in *Google Spain and Google*).[109] If the controller has publicly disclosed such data (or to specific recipients, Article 19 of the GDPR), it has an obligation to take reasonable steps to inform any controllers of the data subject's request to erase such data and any copy thereof.[110] The Modernised Convention 108 recognizes a generic right of erasure when data are processed contrary to the provisions of the Convention (Article 9 (1) (e)). Similarly to rectification, erasure also ensures accuracy, as well as purpose specification. In *Digital Rights Ireland*, the Court considered "the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication" to be an important element of the "the system of protection of the right to privacy established by" secondary law (§32).

The fourth entitlement consists in requesting the restriction of processing (known as 'blocking' in Directive 95/46). Restriction means "the marking of stored personal data with the aim of limiting their processing in the future" (Article 4(3) of the GDPR), for instance by "temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website" (recital 67). Such a restriction can be demanded, pursuant to Article 18 of the GDPR, in cases where the data subject has requested the rectification of their personal data, during the time necessary to verify their accuracy, or similarly when the data subject has objected to processing (see *infra*), during the time necessary to ascertain whether the legitimate interests of the controller can override the rights of the data subject. It can also be requested as an alternative to the erasure of unlawfully processed data, for instance because the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims. In this case, the only processing

[108] The importance of accurate data transcends the field of personal data protection. In the case of *U* (which concerns private life), the ECJ noted that for the information in a "machine readable personal data page of a passport" to be "effectively verifiable by the authorities of those States, the form in which the various components of the name of the holder appear must be free of any ambiguity and, therefore, of any risk of confusion" and therefore "those requirements are not satisfied where, in a passport, the birth name of the holder entered there is indicated by means of an abbreviation which is, moreover, not translated into one of the languages required". Judgment of 2 October 2024 in U, C-101/13, ECLI:EU:C:2014:2249, paragraphs 44 and 47 (2014).

[109] Recital 65 clarifies that such a prerogative is particularly important in the case of data subjects who are, or were, children, at the time of the processing of their personal data.

[110] This obligation, however, has to be commensurate with the costs of implementation and available technology, and must be reconciled with the right of freedom of expression and information, reasons of public interest in the field of public health, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and to fulfil a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

allowed is storage, unless the data subject requests to lift such restriction, or some restrictive conditions apply (Article 18(3)).

The fifth entitlement is new, and consists of "receiving the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided", where the processing is performed on grounds of consent and also by automated means (Article 20 of the GDPR). Although the so-called right to portability does not lay down an obligation to develop interoperable processing systems, recital 68 encourages data controllers to use compatible formats for data transfers, particularly to enable the direct transfer from one controller to the other (Article 20(2)). Article 20 provides for the independence of the right to portability and the right to erasure, which should not be mutually prejudicial.

The final entitlement, already contained in the Directive 95/46 and interpreted by the Court in *Bavarian Lager Ltd.* and *Google Spain and Google,*[111] enables the data subject to object to processing on grounds relating to the particular situation of the data subject, when automated processing relates to the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or to the legitimate interests pursued by the controller[112] or by a third party (Articles 6(1)(e) and (f), and 21 of the GDPR). Pursuant to Article 21 of the GDPR, read in the light of recitals 69 and 70, data subjects are endowed with the prerogative of objecting to the automated processing of personal data consisting in profiling, including for marketing purposes[113] (with limits consisting, for instance, in ensuring public health[114]). The innovation, compared to the corresponding Article 14 of Directive 95/46, is that the former referred to direct marketing, whereas the GDPR refers widely to profiling (based on Article 6(1)(e) and (f)), a point that was anticipated in the discussion on human intervention (*supra*). In this particular connotation, objecting to the processing means allowing an individual not to be characterized solely by a machine. Article 9(1) (d) of the Modernised Convention 108 incorporates these innovations.

The explanation to this attribute is contained in Recital 75, whereby, "… where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles", there is a "risk to the rights and freedoms of natural persons" which could lead to "physical, material or non-material damage".[115]

***

In sum, this attribute takes substance[116] in the control exercised by natural persons on their own personal data, which can be exercised through six different avenues. Such entitlements vary in the degree of intensity, and relate to each other as preliminary and subsequent steps, or alternative steps, of a strategy geared toward controlling one's data. In detail, following access, an individual could resort to restriction with a view to either demand rectification or object to the processing; he or she could request the portability of his or her personal data and, as a more drastic measure, their erasure.

---

[111] See *Judgment of 13 May 2014 in Google Spain and Google, C-131/12, Ecli:Eu:C:2014:317*, § 99.

[112] As for the legitimate interests of the data subject prevailing over those of the data controller, in the context of access to freedom of information, see *Judgment of 29 June 2010 in Bavarian Lager Ltd., C-28/08 P, Ecli:Eu:C:2010:378*, § 77.

[113] Pursuant to Article 6.1(f) and recital 47, marketing is considered a legitimate interest of the data controller, which can nonetheless be overridden as described in the main text.

[114] Recitals 46, 52, 53 of the GDPR.

[115] It is in this light that profiling of children is inadvisable, as they "may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data" (Recital 38 of the GDPR).

[116] Based on the indications of the OHCHR, at validation stage this attribute may need to be split into two.

No case law has, thus far, given indication of the essence. The strongest candidate for the essence is the presence, in the applicable law, of rules which allow to access, at least indirectly (e.g. via the supervisory authority), one's data. Lack of access, in fact, would prevent the right holders from taking any further actions to protect themselves.

Milder candidates for the essence include the existence in the applicable law of provisions enabling to have one's data (at least indirectly e.g. through the supervisory authority) rectified, and the possibility given by the applicable law to challenge profiling, understood as the retention of the individual over his or her identity (and related personality).[117]

5.4 SECURITY AND MINIMIZATION

In §40 of *Digital Rights Ireland* the Court ruled, *a contrario*, that the adherence to minimum safeguards of data security is the essence of personal data. Such a view was confirmed in *Opinion 1/15*, with a slightly different wording that better reflects information security principles used in the GDPR and other instruments of EU law.

Prima facie, the Court derived this understanding of the essence from secondary law, though data security is one of the original FIPs. Yet, it could also be argued that it stems from the right itself, namely either from Art. 8 (1), or from a holistic reading of the right (as proposed by Lynskey). Indeed, the very notion of protection in 'data protection' refers to securing data against risks stemming from processing operations,[118] risks which could lead to more or less severe consequences for data subjects.

If the Court found a provision of secondary law to be the essence, then, *a fortiori*, the principle it refers to can be seen as an attribute. The idea that security can be an attribute is corroborated by the GDPR, where security features among the data protection principles ('integrity and confidentiality'). This finds substance in the expectation of the right holder that the data controller (i.e. the duty holder) implements measures proportionate to the risks of varying likelihood and severity for the rights and freedoms of natural persons (Articles 5(f) and 32 of the GDPR; see also Article 7 of the Modernised Convention 108).

This begs the question of the scope of the attribute of security. A first option is to consider that the essence embodies minimum rules of security, whereas the attribute encompasses the full suite of security measures commensurate to the level of risk,[119] whereby risks are often inherently tied to the nature of the processing.[120] Article 5(f) contains an indicative and non-exhaustive list of the risks, i.e. unauthorised or unlawful processing and against accidental loss, destruction or damage, which is complemented by recitals 75 and 83: for instance, identity theft or fraud, financial loss, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, accidental or unlawful alteration of data, which "may in particular lead to physical, material or non-material damage". Examples of measures to avert risks are provided in Article 32 of the GDPR, and include pseudonymising and encrypting personal data, ensuring the ongoing confidentiality, integrity, availability and

[117] Porcedda, "The Recrudescence of 'Security V Privacy' after the 2015 Terrorist Attacks."

[118] Indeed, secondary law is underpinned by a risk-based approach. Article 29 Data Protection Working Party, "Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks," in *14/EN WP 218* (2014).

[119] I discuss the different notions of risks, particularly with reference to data breaches, in Maria Grazia Porcedda, "Patching the Patchwork? Appraising the Eu Regulatory Framework on Cyber Security Breaches," *Computer Law & Security Review* 34, no. 5 (forthcoming (2018)).

[120] Such as where the processing may: give rise to discrimination, damage to the reputation, or loss of rights and freedoms; concern sensitive information or children; effect profiling; or involve a large amount of personal data and affect a large number of data subjects. Other risks are tied to the security of the data.

resilience of processing systems and services; in case of an accident, swiftly restoring the availability and access to personal data, and regularly testing, assessing and evaluating the effectiveness of technical and organisational measures implemented.

A complementary option is to consider that the attribute of data security includes fulfilling the principle of data minimization, whereby the data processed must be those that are "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5(c) of the GDPR; Article 5(4)(c) of Modernised Convention 108).[121] The rationale for including data minimization in the attribute is that it is intimately connected to security: the fewer the categories of data disclosed by the data subject, the lesser the risks of breaches of security within a single processing operation.[122] Data minimization as part of security also links to accuracy and purpose limitation, in that a suitably carved identification of purposes leads to a more targeted collection of personal data, and also good data cleansing practices. In this last respect, the Court declared in *Google Spain and Google* that "initially lawful processing of accurate data may, in the course of time, become incompatible with the Directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed."[123]

***

This attribute expresses the idea that data should be secured in relation to the risks of varying nature and likelihood entailed by the processing, risks which could lead to physical, material and non-material damage, as well as harm the rights and freedoms of data subjects. It also expresses the legitimate expectation of an individual to be required to communicate the minimum amount of personal data necessary for a given purpose. The attribute fidns substance in the adoption of best organizational and technical practice, but also in the collection of as few data as required upfront, or good data deletion, because data which are not collected are not at risk.

The Court unambiguously stated that the presence of minimum rules ensuring 'integrity, confidentiality and data security' embody the essence of Art. 8.

5.5 CONSIDERATIONS ON SENSITIVE DATA

Bygrave[124] considers the protection of sensitive data as an essential tenet ('core principles') of the right to personal data protection. Thus far, the Court has not directly addressed the matter of sensitive data in the case law on personal data protection. The only reference was contained in *Schwarz*, where the court minimized the risks involved by the use of biometrics. In particular, it declared that "taking two fingerprints "is not an operation of an intimate nature…nor does it cause any particular physical or mental discomfort" and that "The

[121] In previous versions of this study (Porcedda, Cybersecurity and Privacy Rights in EU law. Moving beyond the Trade-off Model to Appraise the Role of Technology (PhD Thesis, European University Institute, 2017)), data minimization was treated as a standalone attribute. The choice made here is justified by the desire to economize the number of attributes that overlap, as opposed to providing the greatest number of nuances.

[122] As I elaborate in Porcedda, "Patching the Patchwork? Appraising the EU Regulatory Framework on Cyber Security Breaches."

[123] *Judgment of 13 May 2014 in Google Spain and Google, C-131/12, Ecli:Eu:C:2014:317*, § 93; "The Recrudescence of 'Security V Privacy' after the 2015 Terrorist Attacks."

[124] Bygrave, *Data Privacy Law*, chapte 5, pp. 145-67.

combination of two operations designed to identify persons may not *a priori* be regarded as giving rise in itself to a greater threat to the rights" in Article 8 (§48 and 49).

From the perspective of identifying attributes, sensitive data cannot constitute an autonomous attribute: to propose the opposite would defy the tenet whereby all personal data deserve protection irrespective of their sensitivity (in relation to the potential risks for the rights and freedoms of data subjects).[125] According to Simitis, the point of sensitive data is to highlight the inefficiency of normally applicable law in ensuring adequate protection, which carries with it the possibility, but not the obligation, of a ban on processing.[126] Rather, sensitive data should be seen as a type of personal data that transversally affects all attributes, and calls for heightened safeguards or a higher threshold for permissible interferences. In this respect, it could be seen as a specification of the rule of law (proportionality) enshrined in the test for permissible limitations: when the interference is potentially greater, the threshold of permissibility is increased.

6 Conclusions

This chapter proposed how to identify the essence of the right to the protection of personal data as understood in EU law, which is a fundamental step in defining the permissible limitations of the right. The essence works as a theoretical border, the trespassing of which leads to the automatic violation of the right.

The approach of the CJEU to the essence in the case law on the protection of personal data which, as stressed several times, remains elusive, may raise more questions than it answers. The reader is left wondering whether the approach to the essence will depend on the nature of proceedings (the clash between an objective of general interest and a fundamental right, as the case of *Digital Rights Ireland* or the reconciliation of two fundamental rights, as the cases of *Coty*) or whether the exercise of the right to an effective remedy is at stake, as in both *Coty* and *Schrems*.

Thus far, the Court seems to have favoured a substantive understanding of the essence of Art. 8, seen as the presence of minimum rules that guarantee the exercise of the right, rules which cannot be omitted or limited. Yet, we cannot discard the case of *Coty*, whereby the essence is not identified in a specific facet of a right, but consists in guaranteeing the exercise of a right *tout court.* In this case, attributes I and II would be fundamental to ensure such understanding of the right, and instrumental in guaranteeing respect for the essence.

It may be possible that both the procedural and the substantive approaches could be used, depending on the issue at stake, or that the Court may find a third way altogether. Pending more enlightening case law by the Court, I have borrowed a methodology developed by the OHCHR in its work on indicators, which aims to identify attributes of rights. This is because, in order to find the essence, it is first of all necessary to trace the contours of the right to the protection of personal data. This exercise builds on the understanding, distilled from case law of the CJEU, that the essence of the protection of personal data can be both a substantive and procedural requirement.

The result of this exercise is summarized in the table below. The first column on the left contains the attribute. The column next to it, on the right, summarizes its content. The last two columns contain a summary of the essence. The first one displays an idea of the essence openly

[125] As stems from the combined reading of the judgments in *Bavarian Lager* (*Judgment of 29 June 2010 in Bavarian Lager Ltd., C-28/08 P, ECLI:EU:C:2010:378*, § 61.) and *Google Spain and Google* (*Judgment of 13 May 2014 in Google Spain and Google, C-131/12, EU:C:2014:317, § 96*).
[126] Spiros Simitis, "Revisiting Sensitive Data," in *Council of Europe* (1999).

identified by the CJEU, whereas the second contains suggestions for core areas that I have identified experimentally. Empty cells correspond to the absence of cores.

Table3 Summary of attributes of the right to personal data protection

Attribute	Description	Essence (CJEU)	Essence – (proposed)
I Legitimate processing (attribute of the rule of law)*	In sum, this attribute refers to the expectation for the data subject that the processing must be legitimate, which refers to three interconnected principles stemming from the rule of law: • Fairness and transparency • Purpose limitation (includes storage limitation) • Lawful legal basis	*Substantive:* Purpose limitation	
Oversight* (II & IV)	It refers to the availability of oversight concerning data processing and the respect of the principles relating to the processing of personal data. It paves the way to two attributes.	N.A.	N.A.
II supervisory authority*	This attribute, which stems from the rule of law, means that the individual can claim without hindrance the intervention of an authority for the protection of his or her right.		Ex post supervision
IV Human interventio n	This attribute means that decisions (significantly) affecting an individual cannot be taken by a machine, and that a human being must be involved in the process		*Substantive:* Obtain human intervention on the part of the controller, to express one's point of view and to contest the decision
III Data subjects' rights	This attribute substantiates the notion of data subjects' control over their personal data, enabling them to intervene in the processing. It includes the following steps, which should be seen as a range of options available to the data subject depending on the situation: • Accessing the data and obtaining a copy • Rectifying inaccurate data • Objecting to processing, including profiling • Restricting the processing of one's personal data • Erasing data • Transferring one's data		*Substantive:* Indirect Access Rectification ? Objection to profiling?
V Security and minimization	This attribute means that the individual can trust that personal information is protected against risks of a varying nature and likelihood which could effect physical, material and non-material damage, as well as expect to communicate the minimum amount of personal data necessary for a given purpose	*Substantive*: the provision of security safeguards in the legal basis	
Sensitive data: affects the threshold of permissible interferences			

* attributes likely to consist of a checklist, and to embody a procedural understanding of the notion of the essence.

In these pages I mentioned that the proposed methodology is experimental; a fully-fledged implementation of the OHCHR methodology to find the attributes requires validation

by a wide community of experts. Moreover, the tenability of the model largely depends on the Court, which has the final word on the nature of the essence.

Nevertheless, this research hopes to open up the debate on both the attributes and the essence, in the belief that the question is too important not to be discussed in the interim. This is because the Court is not the only addressee of this discussion. Having an understanding of the attributes and essence would benefit the analysis of the intrusiveness of technologies on the right to the protection of personal data (and other rights); in this case the addressees are public authorities. Clarifying the notion of attributes and essence would also enable tech companies and their end users (i.e. the addressees) to develop better approaches to so-called 'privacy by design' or, more correctly, data protection and information security by design, which determine, in many ways, the creation of material permissible limitations.[127]

This point calls into question whose standard will prevail: will it be that imposed, *de facto*, by the dominant tech companies? Will it be that imposed by a broad territorial application of the GDPR? Or else, will it be in everyone's interest to find regulatory convergence, thus developing an understanding of attributes and the essence that are acceptable on both sides of the Atlantic, and beyond, hence favouring the approach taken by Bygrave, as well as by Koops et al.? The next few years are likely to determine the answer to these questions, but whichever approach will be better suited to safeguard the right should merit full support.

This point calls into question the 'durability' of the attributes and essence proposed in these pages. Besides the need, called for by the OHCHR methodology, for validation by a wide community, I submit that any definition of the attributes and essence should be conceived with an expiry date. In this respect, I agree with Gellert and Gutwirth, as well as De Hert. Defining once and for all the attributes and essence of the protection of personal data may not be possible,[128] unless we move the clocks back to the early 20th Century. The right's unfixed principles[129] are a direct consequence of the attempt to keep up with with technological disruption (and flow logically from purposive interpretation). One may even look at the architecture of data protection as a matrix, whereby the essence sealed in the attributes stemming from the definition of the right is enriched and enforced by secondary law, and is matched by corresponding principles which express the duties of the data controllers.[130] Such a 'bundle of rights, principles and rules'[131] may not look as elegant as the construction of other rights in the Charter, but is nonetheless worth defending. Safeguarding the independence of Art. 8 as a right endowed with an essence is in fact instrumental in retaining control over one's identity and the free development of one's personality *vis-à-vis* the pressure of a data-driven society, and allow for autonomy to be cherished.[132]

---

[127] Which I discuss in Porcedda, "Privacy by Design in Eu Law. Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection". Note that the attributes and essence defined here concern the right, but by no means the standards necessary for the protection of personal data in a technological environment; for the sake of developing 'by design' approaches, a similar matrix can be created for the duties of data controllers. The most fundamental duties of data controller would correspond to the rights of data subjects, and vice versa.

[128] Gutwirth and Gellert, "The Legal Construction of Privacy and Data Protection."

[129] De Hert, "Data Protection as Bundles of Principles, General Rights, Concrete Substantive Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (Foreword)."

[130] Discussed in Porcedda, "Privacy by Design in Eu Law. Matching Privacy Protection Goals with the Essence of the Rights to Private Life and Data Protection".

[131] De Hert, "Data Protection as Bundles of Principles, General Rights, Concrete Substantive Rights and Rules. Piercing the Veil of Stability Surrounding the Principles of Data Protection (Foreword)."

[132] As I discuss in Porcedda, "The Recrudescence of 'Security V Privacy' after the 2015 Terrorist Attacks."

Acknowledgments. I wish to express my sincere gratitude to the organizers of the 11th edition of the CPDP, in the course of which this chapter was presented. The dialogue with the contribution from one of my co-panelists, Maja Brkan, has enriched this paper. I am very indebted to the anonymous reviewers of this contribution, whose acute remarks led to the substantial improvement of this draft. I also wish to thank Catherine Jasserand-Breeman, Gloria González Fuster, Marta Otto and Olivia Tambou, as well as the editors of this book, for the thought-provoking questions, suggestions of literature and encouragement to publish this chapter. Many thanks, as always, to Martyn Egan for the support in writing the article and linguistic advice. Earlier drafts of this chapter appeared in a project deliverable (2013) and my PhD thesis (2017), partly funded by the FP7 SURVEILLE project (grant agreement no. 284725). Completion of this chapter was funded by the EPSRC research project "Combatting cRiminals In The Cloud" (CRITiCal - EP/M020576/1).