Common Market Law Review **51**: 1–26, 2014.

DATA PROTECTION AND THE LEGITIMATE INTEREST OF DATA CONTROLLERS: MUCH ADO ABOUT NOTHING OR THE WINTER OF RIGHTS?

FEDERICO FERRETTI*

Abstract

EU data protection law is in a process of reform to meet the challenges of the modern economy and rapid technological developments. This study analyses the legitimate interest of data controllers as a legal basis for processing personal data under both the current data protection legislation and its proposed reform. The relevant provision expands the scope of lawful processing, but is formulated ambiguously, creating legal uncertainty and loopholes in the law. The new proposed regime does not resolve the problem. Taking a "rights" perspective, the paper aims to show that the provision should be narrowly interpreted in light of the ECJ case law, and to give effect to the Charter of Fundamental Rights; a rephrasing of the norm is desirable. The provision on the legitimate interest of data controllers weakens the legal protection of data subjects.

1. Introduction and background

Data protection is high on the EU agenda. Article 16 TFEU, in which the principle of data protection is laid down, is included in the "provision having general application" of Title II, alongside other fundamental principles of the EU. It also imposes on the EU legislature the duty of establishing a certain and unequivocal omni-comprehensive legal framework. Moreover, the Charter of Fundamental Rights of the EU has become binding, whose Article 8 normatively recognizes the protection of personal data as an autonomous right distinct from privacy.[1]

* Law Lecturer, Brunel University London, United Kingdom. Avvocato, High Courts of Italy. Member, Financial Services User Group (FSUG). The FSUG was established by the European Commission to advise and provide opinions on the preparation of legislative acts or other policies affecting users of financial services and their practical implementation. The views expressed in this Article are the author's own.

1. But see Protocol 30 of the Treaty of Lisbon regarding the exemption obtained by the United Kingdom and Poland, according to which the Charter of Fundamental Rights will not be justiciable in their national courts or alter their national law.

To meet the challenges of rapid technological developments and the modern economy, the Commission has drafted a proposal in the form of a Regulation (hereinafter "Proposed Regulation")[2] in view of reforming the current legal framework for data protection, Directive 95/46/EC.[3] The declared policy objective is to achieve consistent and effective legal implementation and application of the fundamental right to protection of personal data in all areas of the Union's activities while continuing to guarantee a high level of protection of individuals.

Against this background, it is the aim of this paper to analyse an ambiguous provision that exists both in the current law of Directive 95/46/EC and in the Proposed Regulation, concerning the criteria for making data processing legitimate. It risks representing a loophole in the law and weakening the basis for providing a real protection for individuals (the so-called "data subjects"). This is the so-called "legitimate interest" clause of Article 7(f) of Directive 95/46, which is reproduced in the Proposed Regulation. It provides that:

> "Member States shall provide that personal data may be processed only if:
>
> …
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)."

It thus affirms that those natural or legal persons who determine the purposes and means of the processing of personal data (data controllers) may do so lawfully, without meeting the other tight conditions of the law, if this is necessary for the purposes of their legitimate interest or that of a third party, except where such interests are overridden by the interests for fundamental rights and freedoms of data subjects. It is a processing criterion that expands the scope of permitted processing based on the other legal bases for data processing, in particular consent-based processing. The provision is formulated broadly enough also to address situations of conflicting legitimate private interests of data controllers or third parties *vis-à-vis* the legal right of data subjects, such conflicts requiring the exercise of a balancing test; the

2. COM(2012)11 of 25 Jan. 2012. This was preceded by European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union, COM(2010)609. At the time of writing, the Proposed Regulation is under the scrutiny of the European Parliament and the Council for adoption.

3. Directive 95/46, O.J. 1995, L 281.

Proposed Regulation requires such a balancing from the data controllers. As such, the legitimate interest test provides flexibility to the legal system and it has become a commonly used basis for commercial activities and new technologies that make use of personal data as the "new oil and currency" of the digital economy.[4]

However, if on the one hand flexibility is welcomed by business-oriented supporters, on the other hand it removes a degree of legal certainty, or may even create a loophole in the legal system. This is particularly the case when norms are formulated ambiguously and no guidance is provided. The risks are increased further if these norms do not just need implementation in the various Member States, but also require the exercise of a balancing test between competing interests and/or rights, and consequent interpretation by undefined subjects who are meant to apply the test. The problem is exacerbated when the protection of fundamental rights is concerned, and where such rights aim to safeguard values and freedoms that pertain both to the individual dimension and to the collective sphere in the organization of the democratic order alongside the guarantee for the respect of civil rights, shaping the type of society in which people have decided to live.

The experience of eighteen years of Directive 95/46/EC together with the discussions on the Proposed Regulation have opened the debate in the legislative circles and supervisory authorities as to the re-proposition of the legitimate interest clause in the future regime for the EU. Thus, given the scarce academic intervention on the matter, the ultimate goal of the present article is to make a contribution to the debate on the ambiguous and controversial interpretation and application of the legitimate interest test, as well as its reintroduction in almost identical terms in the new proposed legal framework. It aims to suggest that the current provision should be narrowly interpreted in light of the case law of the Court of Justice, so as to give effect to the Charter which provides that any limitation of the rights it contains must be provided for by law. Likewise, taking a "rights" perspective, it advances the argument that the wording in the Proposed Regulation needs to be modified instead of adding qualifications or requiring delegated acts. This article shows, however, that the fundamental rights element is giving way to economic interests and the promotion of innovation at the expense of those

4. Kuneva, European Consumer Commissioner, "Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling" (Brussels, 31 March 2009), <europa.eu/rapid/press-release_SPEECH-09-156_en.htm>.

values underlying the protection of personal data. It ultimately questions whether the legal discussion has not surrendered to market forces.

To address the issues at stake, this article starts by conceptualizing data protection in light of its current legal status, and attempts to define its underlying values. It purports to show that a reconceptualization and normative separation of data protection from the right to privacy not only reflects more accurately the values that it protects, but also explains the evolutionary path of the rules and principles that need to be taken into account for interpretation, drafting new laws, and more generally shaping policies. Essentially, it gives a basis for evaluating its legal status and for providing an understanding of the solid recognition that data protection has been given in legal instruments and by courts, and which is necessary for the interpretative exercise of the balancing test.

Subsequently, the current EU legal framework is presented alongside the legitimate processing criteria generally, as well as the legitimate interest of the data controllers in particular. It discusses the problematic aspects of the provision and the difficulties surrounding its interpretation and application.

Finally, the paper offers an interpretative approach based on the case law of the ECJ and in light of the Charter. In so doing, it asks whether – despite objective difficulties – the answer to the debate is in fact already known and available through the use in the law of the term "right" instead of "interest" of data controllers, which would make it consistent with the terminology used when reference is made to the fundamental "rights" of the data subjects. However, in the final part, it is noted that the focus of the debate is shifting in a different direction; this analysis brings with it the reflection that in business practice and in the corridors of legislative powers legal rights risk remaining on paper at the expense of market interests and technological innovation.

2. Understanding the concept and values of data protection

Data protection is a complex and multifaceted concept both from a social and a legal point of view. Traditionally, it has been identified with the protection of personal privacy within the context of processing operations involving personal data. However, at least under EU law, the two are distinct, though complementary, fundamental legal rights. They derive their normative force from values that, although at times coincidental and interacting in a variety of ways, may be conceptualized independently.

Even though the recognition of the idea of privacy is deeply rooted in history,[5] as a concept it has been seen as always in transition.[6] It was first developed as an independent legal value when Brandeis and Warren identified it as a tort action, defining it as "the right to be left alone".[7] Since then, it has been largely accepted that in its most general form, privacy protection is a legal way of drawing a line at how far society or other individual subjects may intrude into a person's own affairs. It entails that persons should be able to conduct their personal legitimate affairs relatively free from unwanted intrusions. As such, privacy is an expression of human dignity, development of human personality, and individual freedom.[8] However, modern ideas of

5. Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2002 – An International Survey of Privacy Laws and Developments* (Washington D.C. and London, 2002).

6. Jay and Hamilton, *Data Protection – Law and Practice* (Thomson Sweet & Maxwell, 2003); MacDonald "Myths in the privacy debate" in CEI Staff (Eds.), *The Future of Financial Privacy*, Competitive Enterprise Institute (Washington D.C., 2000), pp. 54–75.

7. Warren and Brandeis, "The right to privacy", 4 *Harvard Law Review* (1890), 193–220.

8. See e.g. Bloustein, "Privacy as an aspect of human dignity: An answer to Dean Prosser", 39 *New York University Law Review* (1964), 962–1007; Stromholm, *Right of Privacy and Rights of the Personality* (Norstedt, 1967); Pennock and Chapman (eds.), *Privacy, NOMOS XIII* (Atherton Press, 1971); Paul, Miller, and Paul (eds.), *The Right of Privacy* (Cambridge University Press, 2000); Rachels, "Why privacy is important", 4 *Philosophy and Public Affairs* (1975), 323–333. Other narrower views of privacy see it as self-determination, intimacy, or a meaningful aspect of interpersonal relationships, personal expression, and choice. See e.g. Parent, "Privacy, morality and the law", 12 *Philosophy and Public Affairs* (1983), 269–288; Gerstein, "Intimacy and privacy", 89 *Ethics* (1978), 76–81; Westin, *Privacy and Freedom* (Atheneum, New York, 1967); Inness, *Privacy, Intimacy, and Isolation* (OUP, 1992); Fried, *An Anatomy of Values* (Harvard University Press, 1970); Gavison, "Privacy and the limits of the law", 89 *Yale Law Journal* (1980), 421–471; Moore, "Intangible property: Privacy, power, and information control", 35 *American Philosophical Quarterly* (1998), 365–378; Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge University Press, 1984); DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, 1997). Such an individualistic approach to privacy has been criticized by scholarship arguing that greater recognition should be given to the broader social importance of privacy: other than a common value in which individuals enjoy some degree of it, privacy is seen as a public and collective value *vis-à-vis* technological developments and market forces, requiring minimal levels of privacy for all. Regan, *Legislating Privacy* (University of North Carolina Press, 1995). There exist also a number of works critical of privacy. The so-called "reductionist approach", for example, takes the view that the right to privacy is derivative, meaning that it can be explained in the context of other rights without meriting any separate attention. As such, it can be protected through other rights without any explicit protection on its own. Any privacy violation is better understood as the violation of other more basic rights: ultimately, the right to privacy is merely a cluster of rights, where these rights always overlap property rights or rights over the person such as bodily security. Thomson, "The right to privacy", 4 *Philosophy and Public Affairs* (1975), 295–314. For another strong criticism of privacy see also Bork, *The Tempting of America: The Political Seduction of the Law* (Simon & Schuster, 1990). These "reductionist approaches" have been criticized by a number of commentators: see Scanlon "Thomson on privacy", 4 *Philosophy and Public Affairs* (1975), 323–333; Inness, op. cit. *supra*;

privacy have been first tested, then shaped, by innovation and the fast development of information technologies and electronic data usage in the last few decades. Today the world cannot be imagined without information technologies. Yet, with the developments and opportunities they bring, the need emerged for new standards that allowed individuals to exercise control over their personal information while permitting innovation and a certain flow of information necessary to support international trade, business, enhanced security, and so on. In practice, there is an unprecedented scale of personal data stored on the internet and used for commercial purposes. Information processing and technologies have a clear potential to influence people's lives dramatically, and this provides an exceptional power in the hands of those who use them, a risk only recently perceived by business and consumer associations alike.[9] Thus, after the landmark definition by Warren and Brandeis other definitions have followed, from the right to control how others use personal information[10] to the vindication of the boundaries protecting individuals' right not to be simplified, objectified or evaluated out of context.[11]

Indeed, data protection refers to the protection of identified or identifiable individuals (data subjects) through the regulation of personal information. Individuals do not own information about themselves. Information does not pre-exist, prior to its expression or disclosure but it is always to some extent constructed or created by more than one agent.[12] Normatively, no copyright or proprietary rights exist on personal information. It pertains to a person, but it does not belong in a proprietary sense to him/her. Those who process personal data (data controllers) have the right to process data pertaining to data subjects

Johnson, "Constitutional privacy", 13 *Law and Philosophy* (1994), 161–193. Another well-known contribution to the "reductionist approach" is that of Posner who made an economic, cost-benefit analysis of privacy. He argued that the types of interests protected under privacy are not distinctive. Most of all, the central proposition is that privacy protection is economically inefficient. Protection of individual privacy is difficult to defend because it does not maximize wealth. With this line of argument, Posner defends organizational or corporate privacy as more valuable than personal privacy, the reason being that the former is likely to improve economic efficiency. Posner, *The Economics of Justice* (Harvard University Press, 1981).

9. London Economics, *Study on the economic benefits of privacy enhancing technologies – Final Report to the European Commission DG Justice, Freedom, and Security* (July 2010), <ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf>.

10. Westin, op. cit. *supra* note 8; see also the landmark decision of the German Constitutional Court *Bundersverfassungsgericht*, Judgment of 15 Dec.1983, 1 BvR 209/83, BVerfGE 65 establishing the right of informational self-determination.

11. Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage, 2000).

12. Rouvroy and Poullet "The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy", in Gutwirth et al. (Eds.) *Reinventing Data Protection?* (Springer, 2009), pp. 45–76.

as long as such processing is lawful, i.e. they abide by procedural rules set by a law whose objective is to protect individual citizens not against data processing *per se* but against unjustified collection, storage, use, and dissemination of the data pertaining to them.[13] As persuasively shown by De Hert and Gutwirth, data protection cannot be reduced to a late privacy spin-off echoing a privacy right with regard to personal data, but it formulates the conditions under which information processing is legitimate. While privacy laws derive their normative force from the need to protect the legitimate opacity of the individual through prohibitive measures, data protection forces the transparency of the processing of personal data, enabling its full control by the data subjects where the processing is not authorized by the law itself as being necessary for societal reasons. In short, data protection law focuses on the activities of the processors and it enforces their accountability, thus regulating an accepted exercise of power.[14]

Like privacy, therefore, data protection finds its roots in the idea that democratic societies should not be turned into societies based on control, surveillance, actual or predictive profiling, classification, social sorting, and discrimination. It is not only a matter of individual liberty, intimacy, integrity, and dignity of individuals but a wider personality right aimed at developing people's social identity as citizens and consumers alike. Hence, one must agree with those concluding that, although "data protection principles might seem less substantive and more procedural compared to other rights … they

13. On discussions about individuals not owning information about themselves, see Kang and Bunter "Privacy in Atlantis", 18 *Harvard Journal of Law and Technology* (2004), 230–267; Rouvroy and Poullet, op. cit. *supra* note 12.

14. De Hert and Gutwirth "Data protection in the case law of Strasbourg and Luxembourg: Constitutionalization in action", in Gutwirth et al.,op. cit. *supra* note 12, pp. 3–44. On a critical view that data protection acts are seldom privacy laws but rather information laws, protecting data before people, see Davis "Re-engineering the right to privacy: How privacy has been transformed from a right to a commodity", in Agre and Rotenberg (Eds.), *Technology and Privacy: The New Landscape* (MIT Press, 1997), pp. 143–165. To appreciate the difference between the two concepts in practice, take the example of a customer of a telephone operator. S/he has given away her/his personal data in order to benefit from the required service. Imagine two different scenarios in the case the customer needs to contact the telephone operator, no matter the reason: a) the customer widely uses the service and s/he is a big spender; b) the customer makes a moderate use of the telephone and spends little money on it. In scenario a) s/he manages to access the operator of the call centre straight away or with little time wait; in scenario b), by contrast, s/he is held on the line for a long time before an operator answers, at times to the point that the customer hangs up the telephone in frustration. The telephone company, without the customer knowing, has invested in software that screens customers' spending and accordingly prioritizes phone calls from those who usually spend more. This would hardly be a violation of the customer's privacy, as s/he has voluntarily provided her/his personal data, including for reasons of customer support. However, many would say that such practice is discriminatory as the telephone company makes an excessive use of data that it already holds or exceeds the purpose for which they were first collected.

are in reality closely tied to substantial values and protect a broad scale of fundamental values"[15] that on many occasions may overlap or intersect but remain separate from those of privacy. For that reason, data protection also has important connotations for society as a whole and it constitutes an important legislative tool to protect a collective social good and fundamental value of a modern democratic order, where citizens freely develop their personality and autonomy. Both privacy and data protection regimes – seclusion and legitimate opacity on the one side, and inclusion, participation, and transparency on the other side – represent a bundle of legal protections and tools to pursue the common goal of a free and democratic society where citizens develop their own personality freely and autonomously through individual reflexive self-determination and for collective deliberative decision making regarding the rules of social cooperation.[16]

From this perspective, granting individuals control over their personal information is more than merely a tool to allow them control the *persona* they project in society free from unreasonable or unjustified associations, manipulations, distortions, misrepresentations, alterations or constraints on their true identity. It is also a fundamental value pertaining to humans to keep and develop their personality in a manner that allows them to fully participate in society without having to make thoughts, beliefs, behaviours or preferences conform to those of the majority or those set from above by the industry for commercial interest.[17] In this sense, the rights conferred by data protection legislation are participatory rights.

There is, however, yet another driving fundamental value that data protection upholds. This is the protection of both individual and public trust, which translates into trust to use new information technology safely, trust in the use of information by public and private agencies, and more narrowly trust in commercial services. Trust and system trustworthiness become the gateway with which to secure users' willingness to depend on a society that is continually evolving, and that relies more and more on information communication technologies in the provision of new forms of governance and services. In an environment where personal data processing is used for an increasing number of purposes, trust may be only generated if technologies are secure, if they are under individuals' control, if personal integrity is respected, and if those making use of personal data are accountable. The proper use of personal data, the guarantee of their protection, and transparency become the means to ensure that trust finds the fertile ground for its roots. In this other sense, thus, the rights conferred by data protection become

15. De Hert and Gutwirth, op. cit. *supra* note 14, at 44.
16. Rouvroy and Poullet, op. cit. *supra* note 12.
17. Ibid.

heterogeneous rights which affect all aspects of human life, from political to consumer rights, as well as technological development.

Notably, both privacy and data protection qualify as distinct fundamental rights rooted in fundamental values, as clearly emerges from the EU legal framework.

3. The EU Legal Framework

Diverging from a static and negative kind of protection, such as that granted under the right to privacy in its expression as the right to respect for one's private and family life, data protection as information law establishes rules on the mechanisms for processing data, empowering individuals to control them. In this way, individuals are allowed to affirm their personality and they can contribute to its formation and expression in a framework of transparency outside the private sphere. Those powers pertain not only to the individuals themselves but also to a public independent authority.[18]

The legal protection of personal data inevitably follows the evolving conceptual shaping of privacy, up to the point of a legal separation of the two under the Treaty of Lisbon.

The legal protection of privacy rights has a far-reaching history. Legal systems in Europe have a tradition of laws on privacy, tort, secrecy and confidentiality. Fascinating as this historical perspective may be, its study is beyond the scope of this work.[19] Narrowing this down to the roots of personal data processing, to understand in depth the fundamental nature of the right to data protection, it is necessary to recall how it was the experience of totalitarian regimes in the 20th century that pushed European nations into attaching great importance to the right to privacy in its modern form. These experiences demonstrated how easily privacy could be abused, and revealed the extreme consequences of such violations.

Privacy was soon elevated to a human right, and at international level was enshrined in the 1948 Universal Declaration of Human Rights. Later, at European level, it was incorporated in the 1950 European Convention for the

18. Rodotà "Data protection as a fundamental right", in Gutwirth et al., op. cit. *supra* note 12, pp. 77–82.

19. See e.g. Banisar and Davies "Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments", 18 *John Marshall Journal of Computer & Information Law* (1999), 1–111; Schober et al., "Transcript: Colloquium on privacy & security", 50 *Buffalo Law Review* (2002), 703–754.

Protection of Human Rights and Fundamental freedoms under the broad protection of one's private and family life, home, and correspondence.[20]

Certainly, the horrors of recent European history and the subsequent international conventions played an important role in the development of data protection laws across Europe[21] and, ultimately, at EU level in the adoption of the Data Protection Directive. Two other factors, however, proved decisive for the enactment of that Directive within the remit of the EU: (i) progressive developments in computers and information technologies, together with the dangers these could represent for individuals, transcending national affairs; and (ii) the need for the free movement of personal data within the Community so as to solve trade disputes arising from separate national regimes, hence the harmonization of data protection laws of the Member States.[22] In the end, the real aims and scope of the Data Protection Directive were both the protection of fundamental rights and freedoms of Europeans *and* the achievement of the internal market. Both objectives were equally important, though in mere legal terms the existence of the Directive, and the jurisdiction of the EU, was based on internal market grounds, with its legal basis in then Article 100a EC (now 114 TFEU).

All the same, in the drafting of the law the EU consistently took a rigorous "fundamental human rights" approach. This stance was particularly important, because it meant that data protection automatically trumped other interests and could not be traded-off for economic benefits.[23]

20. Universal Declaration of Human Rights, 10 Dec. 1948. Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, ETS n. 005.

21. For example, in 1970 the German *Land* Hesse enacted what can be considered the first modern data protection law, which was largely motivated by the growing potential of IT systems combined with the fear of the experience of abuses that took place under the Third Reich before and during the war and the need to prevent their recurrence. Other European countries followed the example with similar national initiatives.

22. See Directive 95/46, Recitals 1–11. A sector specific regime with regard to privacy and electronic communications was the recently amended Directive 2002/58 (the so-called "e-Privacy Directive"), O.J. 2002, L 201 pp. 37–47, as amended by Directive 2009/136, O.J. 2009, L 377/11–36. It is a *lex specialis vis-à-vis* the Data Protection Directive providing for a sector specific regime exclusively applicable to providers of publicly available electronic communication services (e.g. telecom and internet service providers) with regard to the protection of personal data in electronic communications.

23. Case C-465/00, *Rechnungshof* v. *Osterreichischer Rundfunk and Others*, [2002] ECR I-4989. See also Heisenberg, *Negotiating Privacy* (Lynne Rienner, 2005), Ch. 1,2,3; Mayer-Schonberger "Generational development of data protection in Europe", in Agre and Rotenberg (Eds.), *Technology and Privacy: The New Landscape* (MIT Press, 1997), pp. 219–241; Simitis "From the market to the polis: The EU Directive on the protection of personal data", 80 *Iowa Law Review* (1995), 445–469. Indeed, the draft relied heavily on the German and French data protection laws, reflecting views that data privacy could not be traded off against commercial interests or other rights such as freedom of expression. Moreover, there was a strategic element to the choice of labelling data protection as a fundamental human right. The

This position has been made explicit by Article 16 TFEU which, being placed in Title II alongside other fundamental principles of the EU, thus upgrades the provision on data protection to a "provision of general application". It also imposes on the EU legislature the obligation to establish a certain and unequivocal legal framework for data protection. Moreover, with the Treaty of Lisbon, the Charter of Fundamental Rights of the EU has become binding. Normatively, the Charter contains the two distinct rights of "privacy" in Article 7, and the recognition of the protection of "personal data" as an autonomous right distinguished from privacy in Article 8.

4. The legitimate processing criteria and the legitimate interest of the data controllers

In its current form, data protection is a distinctive European innovation in law that over the years has been gaining a mixed fortune outside the EU, from acceptance and emulation in a number of non-EU jurisdictions, to criticism and disputes in others, such as the U.S. The conceptual principles outlined above in this study are reflected in the provisions of the Data Protection Directive, whose scope is to provide for good data management practices on the part of data controllers, that determine the purposes and means of the processing of personal data. The Directive contemplates a sequence of general rules on the lawfulness of the processing of personal data, such as those requiring that data subjects must be informed of the processing,[24] and that the processing must be done for legitimate, explicit and precise purposes, limited to the necessary time-frame (principles of purpose specification and data

ECJ had ruled that it was bound by the constitutional traditions of the Member States and it could not uphold measures incompatible with fundamental rights recognized and protected by the constitutions of those States. According to the ECJ, thus, the EU could not take away the Member States' guaranteed rights, and there was therefore a legal duty not to harmonize at the lowest level in order to avoid conflicts between EU law and the Member States' Constitutions (Case C-11/70 *Internationale Handlelsgesellschaft mbH* v. *Einfuhr – und Vorratsstelle fur Getreide und Futtermittel*, [1970] ECR 1125; Case C-4/73, *Nold KG* v. *Commission*, [1974] ECR 491). Not all Member States approved the so-called "fundamental human rights approach" taken by Directive 95/46. In particular, the UK sided with its business community, complaining that the new standards were much higher than the law existing at the time, mainly maintaining a utilitarian stance and disagreeing about data protection not being traded off for economic benefits. Isolated in its position, the UK abstained from voting on the Directive, signalling to its business community that it had opposed its strict provisions. On the utilitarian approach of the UK, see Kenyon and Richardson "New dimensions in privacy: Communications technologies, media practices and law", in Kenyon and Richardson (Eds.), *New Dimensions in Privacy Law* (Cambridge University Press, 2006), pp. 1–10.

24. Arts. 10 and 11 of Directive 95/46.

minimization), or those granting data subjects the right of access to their data.[25]

Of particular interest here are the legal requirements providing for a valid basis for legitimate data processing. A data controller must be able to provide a valid base for the processing activity only if s/he can claim that the processing relies on one of the criteria established by the law. The set of criteria is exhaustive, so that if a data controller is unable to rely on one of them the processing is unlawful. These are expressed in Article 7 of the Directive:

(a) The data subject has unambiguously given his/her consent.[26]
(b) The data processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.[27]
(c) The data processing is necessary for compliance with a legal obligation to which the data controller is subject.[28]
(d) The data processing is necessary in order to protect the vital interests of the data subject.[29]
(e) The data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.[30]
(f) The data processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are

25. In short, these data protection principles aim at providing that personal data must be:

– processed fairly and lawfully (Art. 6a);
– collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes (Art. 6b);
– adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed (Art. 6c);
– accurate and kept up-to-date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified (Art. 6d);
– kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (Art. 6e).

26. Ibid., Art. 7(a).
27. Ibid., Art. 7(b).
28. Ibid., Art. 7(c).
29. Ibid., Art. 7(d).
30. Ibid., Art. 7(e).

> overridden by the interests for fundamental rights and freedoms of the data subject, in particular their right to privacy.[31]

In the majority of Member States, "consent" is given primary status over the other criteria, in line with Recital 30 of the Directive, which considers it as the first condition to be met for a lawful data processing. However, in some Member States, "consent" is one of several alternatives for data processing, or it is to be relied upon only as a last resort.[32] The reason for the difference in interpretation of the status of consent (i.e. primary versus one of the several equal criteria) lies in the constitutional nature of data protection as privacy or otherwise. In most continental European States, privacy consent has been part of the constitutional doctrine from the development of the concept of privacy as the right to informational self-determination (data protection). By contrast, in those Member States, like the UK, where privacy has not been a constitutional right, the value attributed to consent is seen differently. This may explain the position of treating consent as one of the many alternatives rather than giving it a primary status.[33]

Regardless of possible differences in the implementation or understanding in the Member States, for the purpose of this study it is sufficient to say that all the above criteria present difficulties of interpretation, some of which have been addressed by the Article 29 Working Party or in the literature.[34] These difficulties are unintended outcomes of the EU legislation. They mostly arise from the legal terminology of the Directive and the different legal traditions of the Member States. It would go too far for the purposes of this analysis to examine the multitude of discussions for each of them, be it at EU level or in the various jurisdictions. The Proposed Regulation, due to its legal nature,

31. Ibid., Art. 7(f).

32. The latter, for example, is the view expressed by the UK Information Commissioner available from <www.informationcommissioner.gov.uk>. See also Commission, cited *supra* note 1, 10; Webster, *Data Protection in the Financial Services Industry* (Gower, 2006), p. 24; Carey, *Data Protection – A Practical Guide to UK and EU Law* (OUP, 2004), p. 72.

33. See Korff, "Comparative summary of national laws", *EC Study on Implementation of Data Protection Directive* (Study Contract ETD/2001/B5 3001/A/49), 74; Pinar Manas, "Consent of the data subjects", in *Conference of the Rights and Responsibilities of Data Subjects*, Council of Europe and Office for Personal Data Protection of the Czech Republic (Prague, 14 and 15 Oct. 2004), 67.

34. Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (WP 187, 13 Jul. 2011). The Article 29 Working Party is an independent advisory body on data protection set up under Art. 29 of Directive 95/46; it is composed of representatives from the national data protection authorities of the Member States, the European Data Protection Supervisor and the Commission. It is competent to examine any questions regarding the application of data protection legislation in order to contribute to its uniform application. See also e.g. Ferretti, "A European perspective on data processing consent through the reconceptualization of European data protection's looking glass after the Lisbon Treaty: Taking rights seriously", 2 E.R.P.L. (2012), 473–506.

should provide uniformity and fix the problems of different implementation in the Member States.

However, of the criteria for legitimate data processing there is only one which, as a result of explicit willingness of the legislature, requires interpretation and an exercise of balancing competing interests or rights, leaving the legitimacy of processing to a case-by-case determination without providing any guidance. This is the criterion concerning legitimate interests of the data controller, in Article 7(f), which, albeit in modified terms, is re-proposed in the Proposed Regulation.

The legitimate interest of data controllers or that of third parties is known as the "balance of interest" clause. Data controllers, especially businesses, can process personal data lawfully without meeting the tight conditions provided in Article 7 from (b) to (e) and, most of all, without the consent of individuals under condition (a) of Article 7. Relying on consent may be burdensome for businesses, especially if applied with the high standards set by the Article 29 Working Party, or strictly as a "clear affirmative action" by data subjects as required by the Proposed Regulation.[35] Moreover, new technologies such as data analytics increasingly use large data sets obtained from diverse unrelated sources ("Big Data") which make the obtaining of consent impracticable. Therefore, the legitimate interest clause is considered the criterion upon which the majority of personal data processing takes place, at times the default position, especially for commercial transactions.[36] Under this condition, the processing must be necessary for the purpose, which must be a legitimate interest of the controller or a third party to whom the data is disclosed, provided that such legitimate interests do not impinge upon the fundamental rights and freedoms of individuals. These rights and freedoms are those that require protection under Article 1(1) of the Directive, which contains the key principle underlying the Directive; it represents the very essence of the legislation. The provision affirms that "in accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."

The room for manoeuvre intentionally left by the balance of interest test to national implementation, coupled with the absence of any guidance, has complicated the interpretation and application of the norm, leading to

35. Ibid. See also Recital 25 of the Proposed Regulation.

36. See e.g. the Federation of European Direct and Interactive Marketing, Data Industry Platform, "Proposal for a balanced approach on consent", Position Paper (20 Dec. 2011), at <www.fedma.org/fileadmin/documents/Position_Papers/111220_Data_Industry_Platform_Proposal_for_a_Balanced_Approach_on_Consent.pdf>; Industry coalition for data protection, Paper on Proposals for a new EU legal framework on data protection, at www.bsa.org/~/media/Files/Policy/Security/DataBreach/eudataprotect.ashx.

considerable divergences in the Member States. These inconsistencies go in different directions. For example, the choice of the subject in charge of making the assessment of the test has been left in some countries to the determination of the data controllers, while in others this is for previous specification by the national supervisory authority. Similarly, some countries have provided indications while others have provided none.[37] If anything, Recital 30 of the Directive complicates the picture, as it states that "in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies".[38] In one extreme case, the ECJ has intervened to declare as contrary to EU law the national law restricting the application of the balance of interest criterion only to data in public sources, affirming *inter alia* the direct effect of Article 7(f) of the Directive in case of non-compliance by national law.[39]

Clearly, despite the affirmation of the direct applicability of the legitimate interest test of the Directive, the provision has failed in its goal to create a harmonized legal framework for data processing in the EU. The Proposed Regulation, precisely as it is a regulation and does not require national implementation, is meant to correct the anomaly and create a level playing field within the EU. However, the Proposed Regulation presents once again the test, providing for few changes in the wording but maintaining the substance of the current norm. It reaffirms as a legal ground for data processing the legitimate interest of the controller, and the same balancing test as in the present Directive still needs to be carried out. As an innovation, it drops the indication of third parties' legitimate interests and it requires particular attention in the balancing exercise where the data subject is a child. Also, it excludes the legitimate interest ground where the processing is carried out by public authorities.[40]

37. See Balboni et al., "Legitimate interest of the data controller. New data protection paradigm: legitimacy grounded on appropriate protection", 3 *International Data Privacy Law* (2013), 244–261.

38. Directive 95/46, cited *supra* note 3, Recital 30.

39. Joined cases C-468 & 469/10, *ASNEF and FECEMD* v. *Administración del Estado*, [2011] ECR I-12181.

40. According to Art. 6(f) of the Proposed Regulation, "Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: ... (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks".

The other novelty is that, following the introduction of an accountability principle,[41] it appears that the data controller will be left with the determination of whether it has a legitimate interest to justify the processing, and whether its interest overrides the fundamental rights and freedoms of the data subject. This will correct the uncertainty of the current framework and the different provisions or practices in the Member States. The processing will be subject to supervision, enforcement and, generally, judiciary control.[42]

Nonetheless, in providing further input on the data protection reform discussions, the Article 29 Working Party has urgently argued that additional guidance is essential in order to have a common understanding of the provision, especially as regards the very concept of legitimate interest and where such interest may override the fundamental rights and freedoms of data subjects. Such guidance should occur at EU level, because leaving further regulation to national law through the use of delegated acts would create discrepancies across the Union where data controllers would not be able to process data under the some ground or following the same rules.[43]

The argument is substantial. It is undeniable that, though on the one hand this weighting exercise may confer some flexibility to the system, on the other hand the absence of uniform general rules or guidance inevitably result in lack of legal certainty, especially since Member States are likely to continue to interpret what constitutes a legitimate interest inconsistently and they may well conduct the balance test differently. The issue is exacerbated if one considers that it is not free from controversy that the persons who are deemed to make the balancing and who determine which interests or rights prevail for processing the data are the data controllers themselves, with possible judicial controls only *ex post*. Ultimately and generally, this generates uncertainty with reference to the application of the law and the goal of uniform application in the EU. A loose application of the provision, or the ease of abuse to which it may give rise, is a weakness of the legal system, constituting *inter alia* a possible tool for the circumnavigation of the legal protection offered to individuals, as well as a loophole in the protection of those values behind the law.

41. See Art. 22 of the Proposed Regulation.

42. Article 29 Working Party, "Opinion 08/2012 providing further input on the data protection reform discussions" (WP 199, 5 Oct. 2012).

43. Ibid.

5. Much ado about nothing?

The main problem with the interpretation and application of the provision studied here, regardless of any national implementation or the ECJ decision on its direct effect, is the vagueness of the term "legitimate interests". In particular, in the absence of guidance, there is concern over what kind of interest qualifies as "legitimate" to the point of overriding the fundamental right to data protection and the freedoms it provides. As said, this becomes particularly relevant from the moment that under the Proposed Regulation it is the data controller who undertakes the assessment of the test. The issue is exacerbated by the terminology chosen by the legislature, past and present, which makes use of the term "interest" instead of making a clear reference to conflicting rights.

Notwithstanding the unfortunate terminology used, it is the view of this study that, in its literal meaning, the provision seems to provide that a data controller may process personal data if its interest, or that of a third party, upheld by the law, override those values protected by data protection law analysed above. The whole matter depends on how such an interest is substantiated. Here, an interest means a legally protected interest, i.e. another conflicting right. As seen, the fundamental values behind data protection legislation are particularly important for individuals and society alike, they are based on an unalienable personality right essential for a democratic order, as well as the preservation or promotion of trust. Likewise, data controllers may need to process personal data for prevailing or equally important legally protected values or interests. Therefore, what *prima facie* the provision seems to affirm is nothing new *vis-à-vis* the known distinction between absolute and relative rights, where relative rights are sacrificed if in conflict with an absolute or prevailing relative right, or balanced if a conflicting right of equal nature is counterposed, and where the principles of necessity and proportionality ensure that any interference is kept to a minimum.

Data protection qualifies as a relative right, as confirmed by the latest case law of the ECJ since it has started to recognize data protection as an autonomous right in *Promusicae*,[44] *Rijkeboer*,[45] and *Volker,*[46] albeit not yet

44. Case C-275/06, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU*, [2008] ECR I-271.

45. Case C-553/07, *College van burgemeester en wethouders van Rotterdam* v. *Rijkeboer*, [2009] ECR I-3889.

46. Joined Cases C-92 & 93/09, *Volker und Markus Schecke GbR and Hartmut Eifert* v. *Land Hessen*, [2010] ECR I-11063.

completely separated from the right to respect for private life.[47] The learned judges have stressed that the right to data protection is not absolute, but must be considered in relation to its functions in society. Article 8 of the Charter must be read alongside Article 52(1) of the Charter itself, which states the conditions for legitimate limitations to the Charter rights: "any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others".

The reference in Article 52(1) to the "general interest" is already addressed by Directive 95/46 under the "public interest" condition for processing under Article 7(e), now re-proposed by the Proposed Regulation.[48] According to Directive 95/46, the data processing is justified by reasons of public interest subject to secondary legislation. As Recital 32 confirms, "it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association".[49] At any rate, the concept of legitimate interest cannot be confused with that of public interest[50] but it should rather focus on "the need to protect the rights and freedoms of others" of Article 52(1) of the Charter.

The ECJ has provided precedents of such a balancing of rights. Limiting the analysis on the right to data protection, the latter was balanced with the freedom of expression back in *Lindqvist*,[51] later confirmed in *Satamedia*,[52] emphasizing that it was the responsibility of national authorities and courts to ensure a fair balance between the two. Lately, the balancing exercise was clear

47. On data protection as an autonomous right in the case law of the ECJ see Kokott and Sobotta "The distinction between privacy and data protection in the jurisprudence of the ECJ and the ECtHR", 3 *International Data Privacy Law* (2013), 222–228.

48. Art. 6(e) of the Proposed Regulation.

49. Directive 95/46, cited *supra* note 3, Recital 32.

50. On data protection vs the public interest, see Joined cases C-465/00, C-138/01 & C-139/01, *Rechnungshof* v. *Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauermann* v. *Österreichischer Rundfunk Rundfunk*, [2003] ECR I-4919.

51. Case C-101/01, *Bodil Lindqvist*, [2003] ECR I-12971.

52. Case C-73/07, *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi OY, Satamedia* [2008] ECR I-9831.

in the *Scarlet*[53] and *Netlog*[54] cases, where the ECJ evaluated the relationship between the right to data protection *vis-à-vis* copyright infringement, particularly as regards the disclosure of personal data in order to ensure effective protection of copyright in civil proceedings. The Court concluded that the systematic processing of personal data in the name of copyright enforcement is incompatible with the protection of EU fundamental rights.[55]

Certainly, the balancing test remains far from being an easy assessment, and this is why it should not be left to the unilateral determination of data controllers. Firstly, the application of the test requires a high level of legal expertise, as demonstrated by the case law, which data controllers do not have. Secondly, data controllers would be in a position of clear conflict of interest. Thirdly, they would remain in a situation of uncertainty with the threat of becoming sanctioned *ex post*. Finally, the picture is complicated by the consideration that enforcement is particularly difficult in the area of data protection, since data subjects rarely go to court in the absence of a clearly demonstrable damage and the possibility of actual redress. *Ex post* control, therefore, could be limited insofar as each individual may have little incentive to denounce or sue a data controller, as well as the limited knowledge of the extent of data processing carried out and the underlying technologies by data subjects, who are left in the dark.

Last but not least, it is a requirement of the Charter that any limitation on the exercise of a fundamental right must be provided for by law and respect the essence of those rights and freedoms. By express provision, limitations may be carried out when necessary and if they meet objectives of general interest.[56] Therefore, as recently affirmed by Advocate General Cruz Villalón in his Opinion in *Digital Rights Ireland,* when EU Law provides for interferences with the fundamental rights of citizens, it should define "the principles which must govern the definition, establishment, application and review of observance of the necessary guarantee. It is this very regulation which makes it possible to assess the scope of what the interference with the fundamental right entails in practical terms and which may, therefore, determine whether or not the interference is constitutionally acceptable".[57]

In the absence of regulation of the principles governing definitions and observance of the necessary guarantees, as referred to by Advocate General

53. Case C-70/10, *Scarlet Extended SA.* v. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, [2011] ECR I-11959.

54. Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM)* v. *Netlog NV*, judgment of 16 Feb. 2012, nyr; [2012] 2 CMLR 18.

55. Ibid.

56. Art. 52(1) of the Charter.

57. Opinion of A.G. Cruz Villalón of 12 Dec. 2013 in Joined Cases C-293 & 594/12*, Digital Rights Ireland and Seitlinger and others,* pending.

Cruz Villalón, the only available interpretation of the provision at study is that any conflicting interest of data controllers or third parties should be upheld by the law. Failing that, transferring the argument on the application of the norm, a robust argument could be made that the legitimate interest provision is incompatible with the Charter.

6. The winter of rights

The views expressed above do not seem so straightforward in the current debate on legitimate interests and on the Proposed Regulation. The concept of legitimate interest is all too often viewed as recognizing that data processing involves a balance between the lawful activities of an organization and the impact of data processing on an individual. This understanding captures the day-to-day business of organizations as long as this is lawful. It includes the freedom to acquire wealth under lawful activities. In this perspective, "legitimate" is viewed as in literal dictionary definitions, which assign the meanings of "allowed by law", "reasonable and acceptable",[58] or "conforming to the law or to the rules".[59] Broadly speaking, under this perspective doing business, making profits, and generally the acquisition of wealth are legitimate, as long as the business activity conforms to the rules or is not prohibited by the law.

The case of commercial credit bureaus is paradigmatic. When lenders share consumers' personal financial data via third party commercial entities (credit bureaus) for risk assessment purposes, this is viewed as a legitimate interest. This is the position expressed by the Italian Data Protection Authority for credit risk reduction by lenders in ordinary business, i.e. not the prudential supervision side of sharing information through the Central Bank in the public interest. To appropriately assess applicants' creditworthiness and financial status, i.e. the business risk involved in providing credit, financial institutions share data under their legitimate interest, and commercial credit bureaus process data for profit in the legitimate interest of their clients. It matters little if there is no relationship of cause and effect between the data shared about past behaviour and future credit relationship, or the controversial nature of the type of data shared in order to predict and calculate risk.[60] In any event, the data sharing is to pursue a commercial interest. Indeed, the public interest

58. Cambridge Dictionary at <dictionary.cambridge.org/dictionary/british/legitimate?q=legitimate>.

59. Oxford Dictionary at www.oxforddictionaries.com/definition/english/legitimate?q=legitimate.

60. See Ferretti, *The Law and Consumer Credit Information in the European Community* (Routledge, 2008).

clause is not used, but the clause for private interests. This is despite the explicit recognition by the Italian Authority of the risks for data subjects' fundamental rights in having their private life negatively affected and access to products and services compromised, ultimately impinging on the dignity, reputation, social and professional relations, and private enterprise of individuals.[61]

Similarly, the UK Information Commissioner Office (ICO) by its own admission takes a wide view of legitimate interests, and considers that it is in the interest of other creditors, actual or potential, to make informed decisions. Making informed decisions is certainly a respectable interest, and it is legitimate in the broadest sense. Whether this should prevail over a fundamental right, however, is questionable. The fact that the processing may prejudice a number of individuals is not seen by the ICO as something that necessarily renders the whole processing operation prejudicial to all individuals.[62]

The ECJ's decision in *Asnef and Fecemd* v. *Administración del Estado*[63] indirectly supports this liberal notion of processing of data, having the effect of giving way to the credit industry in the processing of negative financial data of consumers on grounds of their legitimate interest. The case was about national law which qualified the legitimate interest requirement by adding extra conditions, such as that the data should appear in public sources, and thereby excluding, in a categorical and generalized way, any processing of data not appearing in such sources; the ECJ ruled that such national law was precluded.[64] However, the ECJ had the opportunity to touch upon the significance of the legitimate interest where it recognized that the processing of data appearing in non-public sources necessarily implies that personal data is known by the controller, acknowledging that this more serious infringement of the data subject's rights enshrined in the Charter of Fundamental Rights of the EU must be taken into account when balanced against the legitimate interest of the controller.[65] However, it missed the opportunity to make such a balance in the specific case, limiting its analysis to the illegitimacy of the more restrictive criteria imposed by national law. As a result, since the national law

61. Garante per la Protezione dei Dati Personali (Italian Data Protection Authority), "Balancing of interests: data collection by CRAs without consent" (Rome, 16 Nov. 2004), available at www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1671380.

62. Information Commissioner Office, Credit agreements – Data sharing (6 Nov. 2006), at www.ico.org.uk/for_organisations/sector_guides/~/media/documents/library/Data_Protection/Practical_application/CREDIT_%20AGREEMENTS%20-%20DATA_%20SHARING.ashx.

63. *ASNEF and FECEMD*, cited *supra* note 39.

64. Ibid.

65. Ibid. paras. 45–46.

in question prevented commercial credit bureaus from using the legitimate interest clause to process and disseminate consumer financial data within the industry in Spain, the judgment had the factual effect of legitimizing such a practice.

Another example has been offered by Google's merging of data privacy policies across all its services, combining almost any data from any services for any purposes.[66] Google does not collect the unambiguous consent of data subjects and it relies on its legitimate interest to provide, maintain, protect and improve services, develop new ones, and protect itself and its users.[67] If broadly interpreted, Google's justification concerns an interest in itself allowed by the law. The Article 29 Working Party was not satisfied and it filed a complaint letter, where it expects Google to take all necessary steps to ensure compliance with data protection laws and principles. Nonetheless, it was acknowledged that business needs are considered as a legitimate interest for data processing, on condition that the other requirements of the law are respected.[68] The episode shows how easily and generally data controllers may use the legitimate interest justification. It exposes *inter alia* how soft the reaction from supervisors may be to an alleged violation of fundamental rights (a letter containing recommendations: this is hardly a sanction for the violation of a legal right).

Facebook is another fashionable example to take, where the quantity and diversity of personal data processed finds its sole justification under the legitimate interest of the controller for advertising, thus making the service profitable enough to be on offer.[69]

Examples that demonstrate that the legitimate interest has become a common ground to permit data processing may continue at length. However, the point may be already clear that legitimacy can be a very broad requirement which has not been assigned a definite meaning. If coupled with the other

66. Google's Privacy Policy of 1 March 2012, available at <www.google.it/intl/en/policies/privacy/archive/20120301/> replaced by Google Privacy Policy of 27 Jul. 2012, available at <www.google.it/intl/en/policies/privacy/archive/20120727/> replaced by Google Privacy Policy of 24 June 2013 <www.google.it/intl/en/policies/privacy/>. The three policies, which show very few modifications, may be compared at <www.google.it/intl/en/policies/privacy/archive/20120301-20120727/> (comparison between Google Privacy Policies of 1 March 2012 and 27 July 2012), and at <www.google.it/intl/en/policies/privacy/archive/20120727-20130624/> (comparison between Google Privacy Policies of 27 July 2012 and 24 June 2013).

67. Ibid.

68. Article 29 Working Party, "Letter from the Article 29 Working Part addressed to Google along with the recommendations" (Brussels, 16 Oct. 2012), at <ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf>.

69. See Facebook's Redline of the Data Use Policy at <fbcdn-dragon-a.akamaihd.net/hphotos-ak-prn1/851554_458730397568979_663136378_n.pdf>.

pervasive, yet vague, concept of "interest" the result is legal ambiguity and uncertainty.

In discussing the issue that personal data must be collected for "legitimate purposes", the Article 29 Working Party does not prove helpful either. On the contrary, this body considers such a requirement of legitimacy as being in accordance with the law in the broadest sense. It includes all forms of law deriving from all sorts of legal sources. But, within the confines of the law, it includes other elements such as customs, codes of conduct and ethics, contracts, as well as the general context and facts of the case.[70] By express statement, it includes "the nature of the underlying relationship between the controller and the data subjects, whether it be commercial or otherwise".[71]

In the debate over the future European regime and the Proposed Regulation, the latest proposal within the European Parliament has been that the legitimate interest provision could only be relied on in exceptional circumstances, with long prescriptive lists describing in what situations the legitimate interest of the controllers override the rights and interests of the data subjects.[72] Also, data controllers should publish the reasons for believing that their interests override the fundamental rights and freedoms of the data subject.[73] The justification for the proposed amendment results precisely from the quest for clearer guidance and the provision of legal certainty.

However, such a stance has met the criticism of the European Data Protection Supervisor (EDPS) which rejected prescriptive lists because of their counter-productive effect in lacking the flexibility favoured for assessing *in concreto* situations on a case-by-case basis. In contrast, the EDPS welcomes the call for more transparency on the publication of the reasons why the interest of the controller should be prevalent.[74]

Though laudable in their intentions, these initiatives risk complicating the picture even further. For one thing, the idea of listing prevailing interests lacks flexibility for those situations not included or emerging ones, requiring constant legislative updates. In addition, it would not resolve the main concern raised here, which is that interests should not be interpreted as prevailing over

70. Article 29 Working Party, "Opinion 03/2013 on purpose limitation" (WP 203, 2 Apr. 2013).

71. Ibid., p. 20.

72. European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur Albrecht, *Draft Report on the proposal for a regulation of the European Parliament and the Council on the protection of individual with regard to processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012)0011 – C7-0025/2012 – 2012/011 (COD), (Strasbourg, 17 Dec. 2012).

73. Ibid.

74. European Data Protection Supervisor, "Additional EDPS Comments on the Data Protection Reform Package" (Brussels, 15 March 2013).

established rights, unless upheld by the law itself. The dichotomy between interests and rights would find no solution.

Equally, although transparency has to be welcome, the question whether data controllers should be entrusted with the determination of which of their own interest should prevail, albeit forcing them to provide a justification, remains controversial. Likewise, the effort of levelling the imbalance of powers between data controllers and data subjects pursued by the Proposed Regulation would remain frustrated.[75] Ultimately, again, the question as to what extent, and why, an interest should prevail over a legal right remains unanswered.

At any rate, if anything, the debate shows the difficulty, or confusion, to settle a legal definition that, unfortunate as it may be, in reality would be simpler if read in light of the Charter and of the case law. This article has expressed the view that the ECJ case law already provides sufficient guidance and that the legitimate interest should be interpreted restrictively, providing no new extra debate beyond that on the balancing of conflicting rights.

The straightforward solution would be to correct in the Proposed Regulation the anomaly of the current provision by changing "legitimate interests" and "interests" to "rights", wording it thus:

> "(f) the processing is necessary for the purposes of the *rights of* a legal controller *or of a third party*, except where such *rights* are overridden by the fundamental rights and freedoms etc."

instead of the current proposal:

> "(f) the processing is necessary for the purposes of the legitimate interest pursued by a legal controller or of a third party, except where such interests are overridden by the interests of fundamental rights and freedoms etc."[76]

Precedent case law would already offer a direction and the ECJ would remain in charge of carrying the balance. Clearly a degree of uncertainty or discretion would remain, as is always the case whenever rights are balanced. Judicial balancing of rights is far from perfect and has already attracted a large body of academic critique.[77] But at least data controllers would be prevented from, or

75. Recital 34 and Art. 7(4) of the Proposed Regulation.

76. Art. 6(1)(f) of the Proposed Regulation as modified by suggested rewriting.

77. See e.g. de Vries "Balancing fundamental rights with economic freedoms according to the European Court of Justice", 9 *Utrecht Law Review* (2013), 169–192; De Vries, Groussot & Petursson (Eds.), *Balancing Fundamental Rights with the EU Treaty Freedoms: The European Court of Justice as 'Tightrope' Walker* (Eleven, 2012).

limited in, abusing or lawfully circumventing the law, and the spirit of the law and the values that it aims to guard would be better preserved.

Most of all, the provision would be compatible with the Charter and any limitation on the fundamental right of data protection would be provided for by law.

It seems, however, that economic arguments and interests are taking over the legal discussion, where market interests and technological innovation push towards the diminution of safeguards despite the theoretical recognition of the importance of data protection and, on paper, its legal elevation.[78] What the above debate shows is that "rights" are continuing to head towards a period of uncertainty and decline despite the proclaimed intention to strengthen them under the new proposed European data protection regime.

7. Conclusions

This article investigated the legitimate interest of data controllers as a legitimate data processing criterion. The issue is important because it has become a commonly used legal basis for data processing in the commercial area and in new technologies, expanding the scope of processing based on consent. In practice, this legal ground has created a weak basis for providing real protection for data subjects, and it represents a loophole in the current data protection legal framework likely to be reproduced, if not exacerbated, in the proposed new regime. Whilst many of the problems of the current law at EU level are related to the different implementation and interpretation of the data protection Directive in the Member States and they are meant to be corrected by the use of the legal instrument of a regulation, the legitimate interest of the data controllers remains ambiguous, it creates legal uncertainty, and it is likely to undermine the goal of EU-wide uniformity in the application of the law.

Not only there is no guidance in the balancing test, intentionally left to a case-by-case determination, but there is uncertainty over the conduct of the test itself by the same data controllers, which the Proposed Regulation leaves to the self-assessment of the latter, so that data subjects are not in a position to challenge the test effectively.

The most problematic aspect, however, refers to the unfortunate terminology used by the legislature, requiring the balancing of a legitimate interest *vis-à-vis* a fundamental right.

The data processing criterion examined here refers to private interests, not public or general ones addressed elsewhere in the law. If interpreted broadly, a legitimate private interest may lead to abnormal outcomes in the legal

78. See also Rodotà, *Tecnologie e Diritti* (Il Mulino, 1995); Rodotà, op. cit. *supra* note 18.

discourse if weighed against a legal right, even one which is qualified as fundamental. Therefore it is argued that the only possible interpretation has to be restrictive, so that "legitimate interest" is given the meaning "an interest upheld by the law", where relative rights such as data protection may be sacrificed only if in conflict with other absolute rights or prevailing relative legal rights. The ECJ has provided precedents for such an exercise also with regard to data protection conceptualized as distinct from privacy. The Charter, in addition, is explicit in recognizing that any limitation on the exercise of fundamental rights must be provided for by law. In this respect, current conflicting practices endorsed by authorities, interpretations, debates over the new data protection regime, and quests for legislative specifications fail to give to the "rights" element its real significance. The "rights" element, at least in theory, should give data protection a preferred position at least as against those interests that are not characterized as rights or recognized by the law. Equally, data protection as a qualified right protected at the highest legislative rank, such as the Treaty, the Charter, and statutory law, should not be overridden by unqualified interests.

However, economic interests and technological innovations are not only testing the principle but they seem to be driving the debate and the reforming law towards business needs and the weakening of data subjects' protection. The Reformed Regulation has the declared objective to strengthen protection and provide trust in data processing, but it risks leaving a loophole in the law capable of nullifying its goals if the legitimate interest clause is not corrected and rephrased in light of the case law of the ECJ and the Charter.