EUROPEAN REVIEW OF PRIVATE LAW

Wolters Kluwer
Law & Business

Published by Kluwer Law International
P.O. Box 316
2400 AH Alphen aan den Rijn
The Netherlands

Sold and distributed in North, Central and South America by Aspen Publishers, Inc.
7201 McKinney Circle
Frederick, MD 21704
United States of America

Sold and distributed in all other countries by Turpin Distribution
Pegasus Drive
Stratton Business Park, Biggleswade
Bedfordshire SG18 8TQ
United Kingdom

ISSN 0928-9801

This journal should be cited as (2012) 20 ERPL 2

The *European review of Private Law* is published six times per year.
Subscription prices for 2012 [Volume 20, Numbers 1 through 6] including postage and handling:
Print subscription prices: EUR 651/USD 867/GBP 478
Online subscription prices: EUR 602/USD 803/GBP 443 (covers two concurrent users)

This journal is also available online at www.kluwerlawonline.com.
Sample copies and other information are available at www.kluwerlaw.com.
For further information at please contact our sales department at +31 (0) 172 641562 or at sales@kluwerlaw.com.

For Marketing Opportunities please contact marketing@kluwerlaw.com.

The *European review of Private Law* is indexed/abstracted in the *European Legal Journals Index*.
Printed on acid-free paper

EUROPEAN REVIEW OF PRIVATE LAW
REVUE EUROPÉENNE DE DROIT PRIVÉ
EUROPÄISCHE ZEITSCHRIFT FÜR PRIVATRECHT

Founded in 1992 by Ewoud Hondius and Marcel Storme

ISSN 0928-9801

Typeface ITC Bodoni Twelve
Design Dingoj | Peter Oosterhout, Diemen-Amsterdam
Printed and Bound by CPI Group (UK) Ltd, Croydon, CR0 4YY.

European Review of Private Law 2-2012 [473–506] © Kluwer Law International BV. Printed in the Great Britain.

A European Perspective on Data Processing Consent through the Re-conceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously

FEDERICO FERRETTI*

Abstract: EU data protection law is undergoing a process of reform to meet the challenges of the modern economy and rapid technological developments. This study re-conceptualizes data protection in the EU in light of the enactment of the Treaty of Lisbon and the Charter of Fundamental Rights of the EU. It focuses on data subjects' consent as a key component of data processing legislation – alongside the principles of purpose specification and data quality – to reinforce the view that it is a necessary, though not sufficient, tool to guarantee the declared high level of protection of individuals. To prevent confusion, conflation, or abuse of consent and safeguard the fundamental values to which it is tied, this paper puts forward that additional legal constraints and qualifications would be necessary for the enhancement of its application and enforcement. Soft or libertarian paternalism may be the key to nudge individuals towards the desired social outcome while preserving their individual autonomy. The ultimate suggestion is that EU policy makers should take rights seriously and not be seduced by and surrender to conflicting economic interests.

Résumé: La loi européenne sur la protection des données est en train de subir un ensemble de réformes afin de pouvoir faire face aux défis de l´économie moderne et des développements technologiques rapides. La présente étude re-conceptualise la protection des données dans l´UE à la lumière de l´adoption du Traité de Lisbonne et de la Charte des Droits Fondamentaux de l´UE. Elle se concentre sur le principe du consentement comme étant un composant-clé de la législation sur le traitement des données pour renforcer l´idée qu´il est un instrument nécessaire, bien qu´insuffisant, pour garantir le niveau dit élévé de protection des individus. Afin de prévenir la confusion, l'amalgame ou l'abus de consentementet de sauvegarder les valeurs fondamentales auxquelles il est lié, le présent article indique que des contraintes et des qualifications législatives supplémentaires seraient nécessaires pour l'amélioration de son application et de son exécution. Un paternalisme souple ou libertaire pourrait être la solutionpour amener des individus vers le résultat social désiré tout en préservant leur autonomie individuelle. La dernière suggestion est de convaincre les décideurs de l´UE de prendre les droits au sérieux et dene pas se laisser séduire, ou soumettre, par des intérêts économiques incompatibles.

Zusammenfassung: Das EU-Datenschutzrecht befindet sich in einem Reformationsprozess, um den Herausforderungen der modernen Wirtschaft und den schnellen technologischen Entwicklungen zu begegnen. Der vorliegende Beitrag konzeptioniert den Datenschutz in der EU im Licht des Inkrafttretens des Lissabonner

* Lecture in Law, Brunel Law School, Brunel University London. E-mail: fed.ferretti@libero.it or Federico.Ferretti@brunel.ac.uk.

Vertrages und der EU-Grundrechtecharta neu. Er konzentriert sich auf die Einwilligung des Betroffenen als Schlüsselkomponente der Datenschutzbestimmungen – neben den Grundsätzen der Zweckbindung und Datenqualität – und stützt die Ansicht, dass diese ein notwendiges, wenn auch nicht ausreichendes, Werkzeug ist, um das erklärte hohe Niveau von Individualschutz zu garantieren. Der Beitrag führt aus, dass - um Verwirrung, Verwässerung oder Missbrauch bezüglich der Einwilligung zu verhindern und die zu Grunde liegenden grundlegenden Wertungen zu bewahren - zusätzliche gesetzliche Beschränkungen und Bedingungen für die Verbesserung ihrer Anwendung und Durchsetzung notwendig wären. Ein „weicher" bzw. „libertarian" Paternalismus könnte der Schlüssel dazu sein, Individuen in Richtung des gewünschten sozialen Ergebnisses zu lenken und gleichzeitig ihre individuelle Autonomie zu wahren. Schließlich wird angemahnt, dass EU-Politiker diese Rechte ernst nehmen und nicht durch entgegenstehende wirtschaftliche Interessen verführt werden oder diesen erliegen sollten.

1. Introduction

This paper is concerned with data protection legislation in the EU and, in particular, with the meaning and application of the principle of 'data processing consent' in the commercial and consumer protection domain, which may also be used as a possible example for its general application across all areas covered by the law.

Data protection is once again high on the EU agenda. To meet the challenges of rapid technological developments and the modern economy, the EU Commission has launched consultations in view to reform the current legal framework for data protection of Directive 95/46/EC and propose a new comprehensive legislation in 2012. 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.[1]

Data protection has gained significant momentum with the ratification of the Lisbon Treaty. Article 16 of the Treaty on the Functioning of the European Union (TFEU) upgrades the provision on data protection to a 'provision of general application' under Title II alongside other fundamental principles of the EU. It also imposes on the EU legislator to establish a certain and unequivocal omni-comprehensive legal framework for data protection. Equally, the Charter of

1 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*, 4 Nov. 2010, COM (210) 609 final. See also the public consultation at <http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm> followed by a more targeted consultation to the Art. 29 Data Protection Working Party, which provided the opinion WP 168, *infra* at p. 4.

Fundamental Rights of the EU has become binding, which in its Article 8 recognizes the protection of personal data as an autonomous right distinguished from privacy.[2]

Since Article 8 of the Charter of Fundamental Rights of the EU explicitly indicates consent of data subjects as the main basis for a fair data processing for specified purposes, it is envisaged that any new data protection legal framework will not depart from the principle of data subjects' consent as its linchpin, alongside the principles of purpose specification and data quality.

However, as appropriately pointed out elsewhere, if the current European data protection law is flawed, it is reasonable to suggest that the core of the problem lies in the notion and use of consent.[3] Without a doubt, consent is a key element embedded in the current legislation, which has been repeatedly identified as one that needs clarification as to its application and that so far has troubled lawyers as to its meaning and application.[4]

Against this background, the aim of this paper is to reinforce the view that consent of data subjects should indeed remain a key component of data protection legislation as long as its meaning is fully appreciated and, as suggested by EU data protection authorities, it benefits from an improved application and enforcement. However, it will be argued that consent may be easily confused, conflated, or abused. Taken alone, it would be insufficient to guarantee the desired high level of protection of individuals under the current technological developments and the complex business models and practices of the modern economy.

Data protection is a key element in the commercial and consumer domain, whose policies depend significantly on the lawful processing of personal data. Of course, individuals may be concerned as profiled, monitored, or sorted consumers. First and foremost, however, data subjects are the beneficiaries of data protection rights as citizens concerned about their fundamental freedoms in the social and political sphere. Thus, the ultimate focus of this paper is to defend data processing

---

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

3 R. BROWNSWORD, 'Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality', in S. Gutwirth *et al.* (eds), *Reinventing Data Protection?*, Springer, Heidelberg 2009, pp. 83–110.

4 See European Commission, *supra* n. 1; Art. 29 Data Protection Working Party, *The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168 02356/09/EN, adopted on 1 Dec. 2009; European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the 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'*, Opinion of 14 Jan. 2011. See also Commission of the European Communities, *Report from the Commission – First report on the implementation of the Data Protection Directive (95/46/EC)*, Brussels 15 May 2003, COM (2003) 265 final.

consent in the area of consumer protection, as long as it is qualified or supplemented in its application by further normative measures that not only view data protection as grounded in the classical liberal conception of autonomy and individualism but also consider it as a collective good with profound social implications. Such legal constraints, of course, would entail an inherent degree of paternalism to nudge individuals towards the desirable social outcome and away from harm greater than benefits deriving from economic interests.

To reach its goals, this paper is organized in three substantive parts, divided into seven sections.

The first part of the study addresses the concept of privacy and re-conceptualizes data protection in light of the Treaty of Lisbon. In fact, the sharp distinction between data protection and privacy may become important to devise effective policies.[5] Also, it serves the purpose of identifying the ethical or moral values on which data protection is grounded in order to interpret, defend, and reinforce the principles upon which it is based for the changing context posed by the proposed amendments of the existing law.

Data processing consent is explored in the second part of the paper. In particular, it analyses the meaning of true consent to inform its application and enforcement. It aims to shed some light over the illegitimacy or conceptual confusion of current practices that appear to reveal how consent may be easily abused, confused, or conflated to reduce it to a nominal concept that fails to protect individuals adequately. In fact, not only consent may be implied or data processed on the basis of opt-out practices, but it may also be traded for perceived immediate economic advantages, or it may be taken contractually or as part of the general terms and conditions of a contract. Thus, the final part of the paper address the need to take rights seriously, and it proposes to find corrective normative measures for a meaningful consent to inform European policy makers in view of the announced reform of the data processing regime post Treaty of Lisbon.

PART I

2. Data Protection and the Concept of Privacy

Data protection is a complex and multifaceted concept both from a social and a legal point of view. Although data protection has often been identified with the notion of privacy, at least under EU law the two are distinct, yet complementary, fundamental rights. Indeed, as it will be seen, the two derive their normative force from values that, although at times coincidental and interacting in a variety of ways, may be conceptualized independently.

---

5 See S. GUTWIRTH *et al.*, 'Preface', in S. Gutwirth *et al.* (eds), *Reinventing Data Protection?*, Springer, Heidelberg 2009, pp. i–xvi.

Traditionally, the concept of privacy has been seen as always in transition.[6] Nonetheless, the recognition of the idea of privacy is deeply rooted in history.[7] However, it was only in the nineteenth century that the concept of privacy was developed as an independent legal value, when Brandeis and Warren identified such a right as a tort action, defining it as 'the right to be left alone'.[8]

Since that publication, it has been largely accepted that in its most general accession, privacy protection is seen as 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 such a person should be left able to conduct his/her personal legitimate affairs relatively free from unwanted intrusions. As such, privacy is unquestionably considered to be an expression of freedom and dignity of the individual.

There is a considerable body of literature that contributes to the moral, social, political and jurisprudential debates on the concept of privacy. The literature also helps to distinguish between descriptive and normative accounts of privacy. In these discussions, some emphasize the moral value of and interest in privacy, while others focus on it as a legal right to be protected. Some studies have concentrated on privacy as a fundamental value.[9] Others have focused on privacy as human dignity and the development of human personality.[10] Other narrower views of privacy see it as self-determination, intimacy, or a meaningful aspect of interpersonal relationships, personal expression, and choice.[11] Such an individualistic approach to privacy has been criticized by scholarship arguing that

---

6 R. JAY & A. HAMILTON, *Data Protection – Law and Practice*, Thomson Sweet & Maxwell, London 2003; D.A. MACDONALD, 'Myths in the Privacy Debate', in CEI Staff (ed.), *The Future of Financial Privacy*, Competitive Enterprise Institute, Washington, DC 2000, pp. 54–75.

7 Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2002 – An International Survey of Privacy Laws and Developments*, Washington, DC, and London 2002.

8 S. WARREN & L. BRANDEIS, 'The Right to Privacy', 4.*Harvard Law Review* 1890, pp. 193–220.

9 See J. PENNOCK & J. CHAPMAN (eds), *Privacy, NOMOS XIII*, Atherton Press, New York 1971; J. PAUL *et al.* (eds), *The Right of Privacy*, Cambridge University Press, Cambridge 2000; J. RACHELS, 'Why Privacy Is Important', 4.*Philosophy and Public Affairs* 1975, pp. 323–333.

10 See, for example, E.J. BLOUSTEIN, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', 39.*New York University Law Review* 1964, pp. 962–1007: S. STROMHOLM, *Right of Privacy and Rights of the Personality*, Norstedt, Stockholm 1967.

11 See, for example, W. PARENT, 'Privacy, Morality and the Law', 12.*Philosophy and Public Affairs* 1983, pp. 269–288. R. GERSTEIN, 'Intimacy and Privacy', 89.*Ethics* 1978, pp. 76–81; A. WESTIN, *Privacy and Freedom*, Atheneum, New York 1967); J. INNESS, *Privacy, Intimacy, and Isolation*, Oxford University Press, Oxford 1992; C. FRIED, *An Anatomy of Values*, Harvard University Press, Cambridge 1970; R. GAVISON, 'Privacy and the Limits of the Law', 89.*Yale Law Journal* 1980, pp. 421–471; A. MOORE, 'Intangible Property: Privacy, Power, and Information Control', 35.*American Philosophical Quarterly* 1998, pp. 365–378; F. SCHOEMAN (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge 1984; J. DECEW, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, Ithaca 1997.

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.[12] 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 deserving any separate attention. As such, it can be protected through other rights without any explicit protection on its own. Any privacy violation would be better understood as the violation of other more basic rights: ultimately, the right to privacy would merely be a cluster of rights, where these rights are always overlapped by property rights or rights over the person such as bodily security.[13] Another well-known contribution to the 'reductionist approach' is that of Posner who took an economic, cost-benefit analysis of privacy. He argued that the types of interests protected under privacy are not distinctive. Most of all, nevertheless, the central proposition is that privacy protection is economically inefficient. Protection of individual privacy would be difficult to defend because it does not maximize wealth. On 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.[14] Finally, the concept of privacy has attracted also the criticism of feminists who caution that it could be easily used as a shield to cover domination, degradation and abuse of women and other weaker segments of society. In summary, privacy is seen as a dangerous tool to conceal domestic violence and repression of women.[15]

At legislative level, the atrocities of Nazism, fascism, and communism pushed Western nations into attaching great importance to the right to privacy, as it had been demonstrated how easily it could be violated and the extreme consequences of such violations. Privacy was soon elevated as a human right, and its standard at international level was enshrined in the 1948 Universal Declaration of Human

---

12 P. REGAN, *Legislating Privacy*, University of North Carolina Press, Chapel Hill 1995.

13 J. THOMSON, 'The Right to Privacy', 4.*Philosophy and Public Affairs* 1975, pp. 295–314. For another strong critic of privacy, see also R. BORK, *The Tempting of America: The Political Seduction of the Law*, Simon & Schuster, New York 1990. These 'reductionist approaches' have been criticized by a number of commentators: see T. SCANLON, 'Thomson on Privacy', 4.*Philosophy and Public Affairs*, 323–333; Inness, *supra* at 11; J. JOHNSON, 'Constitutional Privacy', 13.*Law and Philosophy*, pp. 161–193.

14 R. POSNER, *The Economics of Justice*, Harvard University Press, Cambridge 1981.

15 C. MACKINNON, *Toward a Feminist Theory of the State*, Harvard University Press, Cambridge 1989. There is not a single version of the feminist critique of privacy. Others, while recognizing that privacy can be a shield for abuse, maintain that privacy should not be completely rejected, e.g., in cases of state imposed sterilization programmes or other abuses. The challenge, in the end, would be that of finding a right balance. See A. ALLEN, *Uneasy Access: Privacy for Women in a Free Society*, Rowman and Littlefield, New Jersey 1988.

Rights and later, at European level, incorporated in the 1950 European Convention for the Protection of Human Rights and Fundamental freedoms (ECHR).[16]

The considerable body of literature on the concept of privacy and the mentioned legislative initiatives all exemplify the difficulty in defining with precision what remains a broad and at times ambiguous term, but it also helps to set the basis for distinguishing between 'privacy' and 'data protection'.

3. The (Re-)conceptualization of European Data Protection

Personal data protection is a distinctive European innovation in law that, over the years, has been gaining acceptance outside the EU. It emerged in the 1970s as a complementary need of the aforementioned ECHR to meet the challenges of emerging technologies. The protection of individuals' personal data also became enshrined in the constitutions and legislation of many continental European countries, which were committed to preventing the reoccurrence of their recent odious histories and the dangerous consequences arising from surveillance of their citizens and intrusion on individual liberties through the use of information technologies. Indeed, in those countries, particularly Germany and France, there was an almost universal consensus to formulate rigid policies to contend with the threats posed by a free and unregulated use and manipulation of personal information.[17]

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 and, ultimately, at EU level in the adoption of Directive 95/46/EC. Two other factors, however, proved decisive for its enactment under the remit of the EU: (i) the progressive development in computers and information technologies, together with the dangers that this could represent for individuals, transcending national affairs; and (ii) the need for the free movement of personal data within the Community to solve trade disputes arising from separate national regimes, hence the harmonization of data protection laws of the Member States.[18] In the end, the real aims and scope of Directive 95/46/EC were (i) the

---

16 Universal Declaration of Human Rights, 10 Dec. 1948. Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 005.

17 For example, data protection is embedded in the Constitutional charter of Spain, Portugal, The Netherlands, Greece, Estonia, Lithuania, Hungary, Poland, Slovenia, Slovakia, and Finland, a stance also taken in other European countries, from Germany to France, and to Italy. See D. HEISENBERG, *Negotiating Privacy*, Lynne Rienner, London 2005, Chs 1, 2, 3; V. MAYER-SCHONBERGER, 'Generational Development of Data Protection in Europe', in P.E. Agre & M. Rotenberg (eds), *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge 1997, pp. 219–241; C.J. BENNETT & C.D. RAAB, *The Governance of Privacy*, The MIT Press, Cambridge 2006, Chs 1, 5; S. SIMITIS, 'From the Market to the Polis: The EU Directive on the Protection of Personal Data', 80.*Iowa Law Review*, 3, 1995, pp. 445–469.

18 See Directive 95/46/EC, Recitals 1–11.

protection of fundamental rights and freedoms of Europeans and (ii) 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 rested on internal market grounds, having its legal basis in then Article 100a of the EC Treaty (now Article 114 TFEU).

Nevertheless, in the drafting of the law the EU institutions 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.[19]

Any possible discussion about this standpoint and its desirability has been recently made explicit by Article 16 TFEU, which elevates the provision on data protection to a 'provision of general application' under Title II alongside other fundamental principles of the EU. It also imposes on the EU legislator to establish a certain and unequivocal legal framework for data protection. Equally, with the Treaty of Lisbon, the Charter of Fundamental Rights of the EU has become binding, and in its Article 8 it recognizes the protection of personal data as an autonomous right distinguished from 'privacy'.

Indeed, data protection refers to the protection through regulation of personal information pertaining to an identified or identifiable individual (data subject). Individuals do not own information about themselves. Information does not pre-exist to its expression or disclosure, but it is always to some extent

---

19 HEISENBERG, *supra* n. 17; MAYER-SCHONBERGER, *supra* n. 17; SIMITIS, *supra* n. 17. 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 European Court of Justice (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 EC 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 EC law and the Member States' Constitutions (*Internationale Handlelsgesellschaft mbH* v. *Einfuhr – und Vorratsstelle fur Getreide und Futtermittel* (C 11/70) [1970] *ECR* 1125, [1972] CMLR 255; *Nold (J.) KG* v. *Commission* (C 4/73) [1974] *ECR* 491, [1974] 2 CMLR 338). Not all Member States approved the described 'fundamental human rights approach' taken by Directive 95/46/EC. In particular, the United Kingdom 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 on the fact that data protection should not have been traded off for economic benefits. Isolated in its position, the United Kingdom abstained from voting on the Directive, signalling to its business community that it had opposed its strict provisions. On the utilitarian approach of the United Kingdom, see A.T. KENYON & M. RICHARDSON, 'New Dimensions in Privacy: Communications Technologies, Media Practices and Law, in A.T. Kenyon & M. Richardson (eds), *New Dimensions in Privacy Law*, Cambridge University Press, Cambridge 2006, pp. 1–10.

constructed or created by more than one agent.[20] Normatively, no copyright or proprietary rights exist on personal information. It pertains to an individual, but it does not belong in a proprietary sense to him/her and those who process personal data (data controllers) have the right to process data pertaining to data subjects as long as such processing is lawful, for example, they abide to 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.[21] As De Hert and Gutwirth persuasively show, 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 necessary for societal reasons. In short, data protection law focuses on the activities of the processors and enforces their accountability, thus regulating an accepted exercise of power.[22]

To appreciate the difference between the two concepts in practice, take the example of a customer of a telephone operator. He/she has given away his/her personal data in order to benefit from the required service. Suppose two different scenarios in the case the customer needs to contact the telephone operator, no matter what the reason is: (a) the customer widely uses the service and he/she is a big spender; (b) the customer makes a moderate use of the telephone and spends little money on it. In scenario (a), he/she manages to access the operator of the call centre straightaway or with a short wait time; in scenario (b), by contrast, he/she is hold 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

---

20 A. ROUVROY & Y. POULLET, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy', in S. Gutwirth *et al.* (eds), *Reinventing Data Protection?*, Springer, Heidelberg 2009, pp. 45–76.

21 On discussions about individuals not owning information about themselves, see J. KANG & B. BUNTER, 'Privacy in Atlantis', 18.*Harvard Journal of Law and Technology*, 2004, pp. 230–267; ROUVROY & POULLET, *supra* n. 20.

22 P. DE HERT & S. GUTWIRTH, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action', in S. Gutwirth *et al.* (eds), *Reinventing Data Protection?*, Springer, Heidelberg 2009, pp. 3–44. On a critical view that data protection acts are seldom privacy laws but rather information laws, protecting data before people, see S.G. DAVIS, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity', in P.E. Agre & M. Rotenberg (eds), *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge 1997, pp. 143–165.

more. This would hardly be a violation of the customer's privacy as he/she has provided voluntarily his/her 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.

These principles are reflected in the provisions of Directive 95/46/EC, such as those that require that data processing must be done for legitimate, explicit and precise purposes, limited to the necessary time frame, which have to be previously notified to the concerned individual (principles of purpose specification and data minimization); or those granting to data subjects the right of access to their data; or, again, those requiring that there should be a valid legal basis for the data processing, such as consent of the data subject, another overriding right, or a legal obligation (the latter two may be summarized under the 'principle of necessity' of the processing, which still needs to be notified to data subjects).[23]

There is a considerable amount of literature available about the perils of an indiscriminate use of information technologies in today's information society. Just to give few examples, it is well known that technologies have the potential capability of aggregating an enormous amount of data in a short time, manipulating, storing, retaining, and disseminating them as quickly to an indefinite number of third parties that may access them from many different points. Then, data may be inaccurate, outdated, out of context, expressed in an unintelligible form, and so on. Consequently, they make it possible to follow an individual's information trail step by step, manipulate his/her economic decisions, profile and/or categorize people, sort and/or discriminate them, impede forgetfulness (the possibility to forget as well as being forgotten), enable people to change and/or progress, infringe (if not stele) their identities, create reputations, and so forth.[24] In practice, today there is an

---

23 In short, the said data protection principles aim at providing that personal data must be:

- processed fairly and lawfully (Directive 95/46/EC – Art. 6a);
- collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes (Directive 95/46/EC – Art. 6b);
- adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed (Directive 95/46/EC – Art. 6c);
- accurate and kept up-to-date; every reasonable step must be taken to ensure that data that 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 (Directive 95/46/EC – Art. 6d);
- kept in a form that 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 (Directive 95/46/EC – Art. 6e).

24 See, for example, C. KUNER, 'Privacy, Security and Transparency: Challenges for Data Protection Law in a New Europe', 16(1).*European Business Law Review* 2005, pp. 1–8; J.D. HANSON & D.A. KYSAR, 'Taking Behavioralism Seriously: Some Evidence of Market Manipulation', 112(7).*Harvard Law Review* 1999, pp. 1420–1572; D.J. SOLOVE, 'The Virtues of

unprecedented scale of personal data left on the Internet or for commercial purposes. Data may be easily disseminated and/or databases may be created, which may undergo data mining techniques. Accordingly, the ways of collecting personal data have become increasingly elaborated and less easily detectable.[25] For example, they can be used for targeting certain individuals or excluding others from certain products or services (marketing), they can be used for making risk assessments about dealing with certain individuals and on what terms, they may be used for tailored pricing, and so forth. In soft cases, consumers may be annoyed for receiving unsolicited offers or having their e-mail inbox full of undesired commercial messages; more seriously they may feel offended for having been profiled as persons different from their perceived real self, they may be offended for not being treated as other customers or classified at a lower level (e.g., in the case of scoring) or ignored, even worse they may be forced to pay more than others for the same products or services (such as for telephone or Internet facilities or utilities), or worryingly they may be even excluded from certain products or services (e.g., from obtaining online facilities, credit, a mortgage, a particular product, or even a to rent a home). It is undeniable that such forms of actual or predictive profiling, classification, or discrimination may lead to serious social consequences and problems also when applied in the commercial sphere.

In short, information processing and technologies have a clear potential to influence dramatically the lives of people, 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.[26] Like privacy, therefore, data protection finds its roots in the idea that democratic societies should not be turned into societies resting on control, surveillance, actual or predictive profiling, classification, social sorting, and discrimination. It is not only a matter of individual liberty, intimacy, and dignity of individuals but a wider personality right aimed at developing people's social identity as citizens and consumers alike. Hence, it has to be agreed with the conclusion that, although 'data protection principles might seem less substantive and more procedural compared to other rights *(…)* they are in reality closely tied to substantial values and protect a broad scale of fundamental values'[27] that on many occasions may overlap or intersect but remain separate from those of privacy. For that reason, it also has important connotations for society as a whole, and it

---

Knowing Less: Justifying Privacy Protections Against Disclosure', 53.*Duke Law Journal* 2004, pp. 967–1062; S. RODOTÀ, *Tecnologie e Diritti*, Il Mulino, Bologna 1995; M. LEVI & D.S. WALL, 'Technologies, Security, and Privacy in the Post-9/11 European Information Society', 31(2).*Journal of Law and Society* 2004, pp. 194–220.

25 See, for example, European Commission, *supra* n. 1, and London Economics, *Study on the economic benefits of privacy enhancing technologies – Final Report to the European Commission DG Justice, Freedom, and Security* (July 2010).

26 *Ibid*.

27 DE HERT & GUTWIRTH, *supra* n. 22, p. 44.

constitutes an important legislative tool to protect a collective social good and fundamental values of a modern democratic order where citizens freely develop their personality and autonomy. Therefore, both privacy and data protection regimes (i.e., seclusion and legitimate opacity on the one side, and inclusion and participation 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.[28]

From this perspective, granting to individuals' control over their personal information is not only a tool to allow them control over the *persona* they project in society free from unreasonable or unjustified associations, manipulations, distortions, misrepresentations, alterations or constraints on their true identity but 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 conform thoughts, beliefs, behaviours or preferences to those of the majority or those set from above by the industry for commercial interest.[29] In this sense, the rights conferred by data protection legislation are participatory rights of informational self-determination, where the requirement of individual consent for the processing of data is the cornerstone unless the processing is *necessary*, subject to notice to data subjects pursuant to Articles 10 and 11 of Directive 95/46/EC, for the performance of a contract to which the data subject is party, for compliance with a legal obligation of the data controller, to protect a vital interest of the data subject himself/herself, for public interest, or for overriding rights of the data controller or third parties.[30] As such, the instrument of consent as the tool to grant such participatory right rests on the expression of a classical liberal conception of autonomy and individualism.

However, as the next section will attempt to demonstrate not only that the instrument of consent may be easily misused or abused but also that placing the focus exclusively on individual autonomy to protect a collective good may jeopardize or hamper both effective self-determination of individuals and the realization of the social values and benefits upheld by data protection rights. This element may prove crucial in view of the proposed reform of the current EU legal framework for data protection.

---

28 ROUVROY & POULLET, *supra* n. 20.

29 *Ibid*.

30 Directive 95/46/EC, Art. 7(b) Directive.

PART II

4. Data Processing Consent

The issue of consent is a complex one that raises difficult questions in many areas of the law. As such, it has attracted specific attention in its own right.[31]

At European level, Article 8 of the Charter of Fundamental Rights of the EU explicitly recognizes consent of data subjects as the main condition to enjoy the fundamental right to the protection of personal data:

> [e]veryone has the right to the protection of personal data (…) and 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 [emphasis added]

Likewise, the central legal requirement under the current legal framework set by Directive 95/46/EC is that personal data must be processed fairly and that, in the absence of another necessary basis set by the law, the 'unambiguous consent' of the data subject is the central ground for processing, which empowers the data subject in the control over his/her data and in his/her self-determination.[32] The Directive's definition of consent is limited to 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.[33]

The EU Commission has recognized that the 'notion of "unambiguous consent" (Article 7a) in particular, as compared with the notion of "explicit consent" in Article 8, needs further clarification and more uniform interpretation'.[34] In maintaining their duty to transpose the provisions of Directive 95/46/EC into domestic law, the Member States – with the exception of the United Kingdom – all allow for the processing of personal data on the basis of consent in terms almost identical to those used in the Directive or at least close to it with some additional requirements.[35] Moreover, in the majority of countries consent is given

---

31 See, e.g., D. BEYLEVELD & R. BROWNSWORD, *Consent in the Law*, Hart, Oxford 2007.

32 Article 7(a) of Directive 95/46/EC.

33 Article 2(h) of Directive 95/46/EC. Recital 30 of the Directive, in turn, simply defines consent as an expression of the will of the data subject.

34 Commission of the European Communities, *supra* n. 4, p. 17.

35 Overall, there is substantial convergence between the continental European States on the basic definition of consent or at least on its application in practice. For example, the data protection laws of Austria, Belgium, Cyprus, Czech Republic, Denmark, Finland, Greece, Latvia, Lithuania, Luxemburg, Malta, The Netherlands, Poland, Portugal, Slovakia, Spain, and Sweden word the definition of consent in more or less exactly the same terms as the Directive. German law requires that consent should be given in writing, while Italian law stipulates that consent should be documented in writing. By contrast, UK law does not define consent, and the data protection

primary status over other criteria. This appears in line with Recital 30 of the Directive that considers consent as the first condition to be met for a lawful data processing. However, in countries such as the United Kingdom, consent should be relied upon only as a last resort.[36] This different interpretation is deemed to reflect the different conception that in most continental European States data protection is based on constitutional principles, and consent – as its essential component – has been a part of the constitutional doctrine of these States ever since the concept of the right to information self-determination took shape.[37]

Three key elements may be identified in Article 7 of the Directive, which should form the backbone of every domestic implementation of the notion of 'consent': (i) it must be unambiguous, as ambiguous consent does not preclude all doubts that the data subject has expressed his/her will, and therefore it is not consent; (ii) it must be freely given, as enforced consent obtained under coercion, undue influence, or pressure is no consent; (iii) it must be specific and informed so that all processing activities are properly described, as uninformed or vague consent is no consent.

At least, these elements seem to shed some light over the illegitimacy of assumed or implicit consent and some practices making use of it. This seems the view taken by the large majority of Member States that require for any consent to be manifest. Likewise, such a consent seems to be not admissible for the purposes of data protection inasmuch as the data subject must express his/her will unambiguously for such an expression to be clear and conclusive.[38] A non-response by a data subject is ambiguous as long as specific information is not provided and no option has been given to freely decide whether agreeing or not. Arguably, therefore, consent should clearly emanate from the data subject in a way that no doubts exist over his/her agreement, whatever form it takes, oral or written.[39]

---

authority on occasions relates the nature of the consent required to the circumstances, while elsewhere it expressly refers back to the Directive in its guidance on the law. See Commission of the European Communities, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States* (Brussels, 16 May 2003), 10; D. KORFF, 'Comparative Summary of National Laws', *EC Study on Implementation of Data Protection Directive* (Study Contract ETD/2001/B5 3001/A/49), p. 27; J.L. PINAR MANAS, 'Consent of the Data Subjects', in *Conference of the Rights and Responsibilities of Data Subjects*, The Council of Europe and the Office for Personal Data Protection of the Czech Republic (Prague, 14 and 15 Oct. 2004).

36 WEBSTER, *Data Protection in the Financial Services Industry*, Gower, Aldershot 2006, p. 24; P. CAREY , *Data Protection – A Practical Guide to UK and EU Law*, Oxford University Press, Oxford 2004, 72.

37 See KORFF, *supra* n. 35, p. 74; PINAR MANAS, *supra* n. 35, p. 67.

38 Commission of the European Communities, *Analysis and impact study on the implementation of Directive EC 95/46 in Member States* (Brussels, 16 May 2003), p. 10; WEBSTER, *supra* n. 36, p. 24; CAREY, *supra* n. 36, p. 72.

39 This view has been shared explicitly by the Data Protection Authorities of the Member States. See KORFF, *supra* n. 35, pp. 74–78; PINAR MANAS, *supra* n. 35, pp. 67–74. The United Kingdom

However, despite such an apparently robust legal protection accorded to data subjects, consent may be obtained by a number of methods and has proved problematic as a basis for personal data processing as it could be easily abused, confused, or conflated. This is particularly important because in theory a consent that does not meet the requirements of the law or that is vitiated should be regarded as void, invalidating all data processing *ex tunc*.

5. Abused, Confused, or Conflated Consent

There are many instances, particularly in commercial transactions, where the empowerment of consumers and the nature of 'data processing consent' may not always be properly applied or is often confused. Also, there are many situations where there is a clear unbalance between the consumer (data subject) and the business counterpart (data controller).

Moreover, the complexities of some business models, data collection tools and practices, vendor/customer relationships and/or technological applications may make it impossible for consumers to understand or freely and actively decide to accept the consequences of consenting to the processing of data, particularly when faced by perceived immediate economic or other benefits in kind. In practice, these occurrences happen not only in the context of online transactions but also, more generally, in the inclusion of notices of data processing consent in the standard terms of contract for the purchase of goods or services, whether online, on hard paper, or verbally.

A known online phenomenon is that of consent by opt-out, which enables the automatic processing of data unless a data subject explicitly objects to such data processed (i.e., he/she opts-out). In light of the proposed amendments to the EU data protection legal framework, it is now accepted and recommended that, as far as information and communication technologies in the consumer domain are concerned, the optimal solution is to counterbalance the benefits of technological advancements and risks for individual data protection by complementing the legal framework with the principle of 'privacy by design': accordingly, data protection safeguards should be incorporated in the design and operation of technologies and systems so that they will become default settings and new legal norms will provide for such binding requirement for technology designers and producers, as well as for data controllers. Hence, opt-in consent will become a key explicit element that

---

once more provides an exception. Guidance on the law, issued by the data protection authority, suggests that consent may, in certain circumstances, be implied. According to KORFF (p. 75), this interpretation is doubtful in terms of compliance with the Directive, which requires that the data subject's agreement to any processing be 'signified'. The author suggests that, presumably, the UK data protection authority's guidance must be read as meaning that a data subject's consent can be inferred from signals which imply his agreement, even though such signals may not be very explicit.

permits the processing of personal data by data controllers that would otherwise be forbidden.

However, treating consent as a transactional moment, using standard form or click-wrap agreements, may constitute a mechanical or pre-functionary means of obtaining overarching consent for data processing. The inclusion of data processing consent in the general terms and conditions of sale or services can be a common, yet subtle or elusive, method of obtaining consumer consent notwithstanding whether a transaction occurs online and irrespective of the opt-in/opt-out dichotomy. As the voluntary element is central to agreeing to something, consent becomes associated with the legal paradigm of contract. Acceptance of a contract by a consumer automatically signifies acceptance of a term or condition in a clause of the contract whereby the consumer contextually agrees for the processing and/or communication to third parties of his/her personal data.

At this stage, a key distinction should be made: there are certain personal data that are necessary for the performance of the 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 the contract. For example, in bank transactions, if a consumer wishes to open a current account, there are some data that are essential and necessary for the performance of the contract without the processing of which the service and related products, including a debit card, could not be given. This is a circumstance already considered by the Directive, which in Article 7(b) states that the processing is fair provided that data subjects are informed of such processing. No consent would be required as the processing would fall within the other necessary conditions set by the law itself. In this case, such notice could well be placed in the terms and conditions of the contract. However, there are other data processing activities that, although motivated by asserted economic benefits, are not strictly necessary for the performance of the contract or to take necessary steps prior to entering the contract. In practice, data controllers may be tempted to maximize data collection and use for purposes beyond a necessary processing likely to have excessive scope or deep use conditions. In the above example, for instance, this would happen if a bank decided to use the personal data for marketing purposes and introduced a clause that acceptance of the agreement allowed the use and communication of personal data for marketing purposes. This is a simple example portraying an obvious situation, but with the use of today's technologies and complex business organizations, there may be less obvious situations where personal data are used and database created even if the proper notice is served to data subjects.

Arguably, however, an implicit or a contextual consent to data processing by consenting to the general terms and conditions of sale or service does not necessarily lead to unambiguous consent as required by Article 7 of Directive 95/46/EC. On the contrary, the concepts of 'data processing consent' and 'agreement of contractual terms' may be often confused or conflated. Thus, although the main principles of data protection, together with the introduction of additional principles such as 'privacy by design', may still be valid to respond to the needs of participatory

informational self-determination *vis-à-vis* the challenges posed by increasingly sophisticated business models and customer relations, this would be far from being a desirable application and enforcement of the existing data protection principles in practice.[40]

Accordingly, consent offers a procedural justification of the values and rights that data protection aims to promote and guarantee. If such rights have to be taken seriously, the abuse, confusion or conflation of consent should be avoided.[41] An understanding of the requisites of what constitutes a true data processing consent may therefore be helpful to shed some light over what would be necessary to ensure the standards governing its application and avoid the danger that it remains just a notional concept.

6. The Requisites of a True Consent

A major interpretative challenge is that of establishing the conditions for giving a valid consent in the context of, and according to, data protection legislation.

6.1. Informed Consent

The primary prerequisite for the validity of consent according to Article 2(h) of the Directive is that it must be informed. Again, if one looks at contract law, the question of how much information is needed before a party's consent is sufficiently informed to enter validly into a transaction is one that has troubled academic commentators for a long time.[42] Actually, information asymmetry has informed a great deal of consumer legislation. What has to be looked at here, however, is the information to be given to data subjects pursuant to Articles 10 and 11 of Directive 95/46/EC. The issues relating to the disclosure notices in data protection terms raise additional complex questions on their own that would require a separate analysis. What needs to be stressed here is that data subjects must be properly and effectively informed, before the collection of the data, of the specific circumstances of the processing (its purpose, the identity and details of the recipients, all the logics behind data processing, the consequences, the valuation standards and decisions resulting from personal profiles, possible sharing of data and the actors involved, and so on). Such a notice must be precise and intelligible to the data subject. Consumers must understand the facts and implications of an action to be able to make informed choices, ensuring that they are effectively able to choose freely and voluntarily whether or not to take part into an agreement and/or in additional processing activities of their data for purposes not strictly necessary to the subject matter of the agreement. Moreover, data protection notices have the essential function of promoting transparency allowing data subjects to maintain control over

40 As envisaged by the Art. 29 Data Protection Working Party, *supra* n. 4.

41 See BROWNSWORD, *supra* n. 3.

42 BEYLEVELD & BROWNSWORD, *supra* n. 31, p. 9.

information relating to them. For all these reasons, therefore, it may be maintained that data processing notices should disclose also the data mining and manipulation techniques that may be employed, as well as the data aggregation procedures that may be in place. To what extent these may be intelligible to average data subjects remains an open question.

6.2. The Difference between Data Processing and Contractual Terms

The consent to process personal data for the specific purposes of the contractual relationship between the parties of a contract should be distinct from the legitimization of business organizations processing consumers' data for purposes related, but not essential, to the supply of goods or provision of services that are the subject matter of the underlying agreement. The former processing, in fact, would be necessary in order to conclude and continue the business transaction *per se*, which is a processing separate from that of additional activities, even when these are ancillary to the principal relationship. As it would be necessary for the performance of the contract, it falls within the scope of Article 7(b) of the Directive and does not require consent. This leads to the important consideration that, in consumer transactions, account may be taken of more than one type or instance of consent of the consumer/data subject: the consent that is a requisite for the conclusion of the legal dealing between a supplier and a consumer (the contract) and the consent of the consumer regarding the processing of his/her personal data. This means that consent, for the processing of those data not covered by the necessity principle of Article 7(b), cannot be given by accepting the general terms and conditions for the service that he/she requires.[43] This is also a corollary of the rule that 'consent' for data processing must be specific ex Article 6(b).

In principle, the rights conferred by the data protection legislation are enjoyed by a data subject independent of the package that has to be negotiated with a supplier of goods or services, precisely in the same fashion described by Howells and Weatherill with regards to the rights conferred to consumers by consumer legislation or those enjoyed by workers under employment law.[44]

Also, the function of consent in data protection is different from its function in contract: in the former instance, it represents a permission for what would otherwise be a violation of a data subject's right or, as defined by Brownsword, a

---

43 PINAR MANAS, *supra* n. 35, p. 76. See also Art. 29 Data Protection Working Party on Data Protection, *Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC*, 11601/EN WP 90, adopted on 27 Feb. 2004. According to Art. 7(b) of the Directive, personal data may be processed if the 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.

44 G. HOWELLS & S. WEATHERILL, *Consumer Protection Law*, Ashgate, Aldershot 2005, pp. 14–18.

procedural justification for the underlying right;[45] in the contractual type of consent, by contrast, the function of consent would not be to give to one party a defence against the breach of the other party's rights, but it functions instead to create new rights and duties in the relationship between the parties.[46]

A thorough account of the reasons behind the importance of consent in contract law is provided by Smith, according to whom two possible explanations exist: (i) consent matters because it is a prerequisite for establishing responsibility, and responsibility is a prerequisite for legal liability; (ii) preferably, consent matters because a non-consensual contract may give rise to an unjust enrichment.[47]

Arguably, none of the two suggestions would apply to consent under the data protection law, unless one considers personal data exclusively as a commodity neglecting the rationale and justification of data protection. Indeed, advocates of the view that there may be a contractual relationship between the data subject and the data controller support the idea that individuals have proprietary rights on their information, which constitute an asset in the information society and therefore may be the object of economic transactions.[48]

As seen, however, the conceptualization of data protection derives its normative force from fundamental values and freedoms and not from property. Data processing consent, therefore, would be best viewed as a unilateral act, which would make it more consistent also with the fact that in the law it is neither always necessary nor always sufficient.[49]

Unlike in private law, thus, data processing consent would be best understood as providing an ongoing act of agency to the data subjects rather than

---

45 BROWNSWORD, *supra* n. 3.

46 BEYLEVELD & BROWNSWORD, *supra* n. 31, p. 7. The authors specify that particularly in consumer contracts, the law requires that consent should be free and informed, thus suggesting that the law might set the same conditions for consent irrespective of the function played by consent.

47 S.A. SMITH, *Contract Theory*, Oxford University Press, Oxford 2004, pp. 324–331.

48 See, for example, S. BIBAS, 'A Contractual Approach to Data Privacy', 17.*Harvard Journal of Law and Public Policy* 1994, pp. 591–605; P. MELL, 'Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness', 11.*Berkeley Technical Law Journal* 1996, pp. 1–92; J. LITMAN, 'Information Privacy/Information Property', 52.*Stanford Law Review* 2000, pp. 1283–1312; A.R. MILLER, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, Ann Arbor, Chicago 1971, p. 21; P.M. SCHWARTZ, 'Property, Privacy, and Personal Data', 117.*Harvard Law Review* 2004, pp. 2055–2128; V. BERGELSON, 'It's Personal but Is It Mine? Toward Property Rights in Personal Information', *U.C. Davis Law Review* 2003, pp. 379–451; A.D. MOORE, 'Toward Informational Privacy Rights', 44.*San Diego Law Review* 2007, pp. 809–845; J.E. COHEN, 'Examined Lives: Informational Privacy and the Subject as Object', 52.*Stanford Law Review* 2000, pp. 1373–1437; P. SAMUELSON, 'Privacy as Intellectual Property', 52.*Stanford Law Review* 2000, pp. 1126–1171.

49 D. SOLOVE, 'Conceptualising Privacy', 90.*California Law Review*, pp. 1087–1154; ROUVROY & POULLET, *supra* n. 20, pp. 72–74.

an isolated moment of contractual agreement when the parties communicate their intention to be bound by a specific agreement.[50]

In summary, in contract law the consent of the individual is necessary to conclude the contract and obtain the service that he/she requests. By contrast, in the 'consent' required for the legitimate processing of data that do not fall within the scope of Article 7(b) of the Directive, the data subject's consent does not have the element of causal necessity for the activity and purpose of the data controller with whom he/she intends to enter into an agreement. After all, the issue of the processing of personal data that are not strictly necessary for a given circumstance is not unknown to data protection: indeed, it is the one that justifies the use of consent ex Article 7(a) of the Directive separately from the underlying transaction or operation ex Article 7(b) of the Directive.

6.3. Freely Given Consent

Another fundamental feature is that, as a general rule, each instance of consent should be the free choice of the individual. Arguably, in fact, in data protection terms consent would be meaningless if people have no option but to consent in order to obtain a benefit or a service that could be provided nonetheless.

The conditions for a free and voluntary consent lead to the very essence of its meaning, which has to be examined within the context in which it is provided.

As seen, the expression of will, in order to be regarded as having been given voluntarily, must refer explicitly to the processing of personal data, and not to the consent to conclude the principal contract. This would already be a sufficient reason to maintain that the refusal by a data subject to permit an amount of processing of personal data that is not necessary for the provision of a service that he/she requires should not mean that he/she is failing to consent to that service. Or, again within the category of data that does not fall within the 'necessity principle', it may well be the case that someone may agree with the processing of some data but not certain other data. A typical example is that of commercial marketing: no one denies that it is an important economic activity that would increase the profitability of an industry, this latter circumstance possibly being reflected also in an economic advantage for consumers. It is well accepted in data protection, however, that data controllers may not obtain the giving of the consent to process the data for such a purpose upon the understanding that the goods or services may not otherwise be purchased or obtained. According to the Directive and read in conjunction with the

50 See also I. KERR *et al.*, 'Soft Surveillance, Hard Consent – The Law and Psychology of Engineered Consent', in I. Kerr *et al.* (eds), *Lessons from the Identity Trail*, Oxford University Press, Oxford 2009, Ch. 1.

proportionality principle, such a practice to obtain consent would lack its freely given element.[51]

However, some may reasonably contend that this application would contrast with the basic principle of 'freedom of contract', which is an issue related but different from the incorporation of data processing consent in the terms and conditions of contract. For example, it could be suggested that if data subjects do not accept data controllers' processing and own procedures, albeit a separate request for consent, thus failing to consent according to Article 7(a) of the Directive, then data controllers would be free to refuse to enter into a contract that would leave the data subject without the good or service required. Either a data subject accepts to provide such a permission or a commercial organization should be free to avoid any business with him/her. After all, parties of a contract and commercial organizations, in particular, do not have any obligation to enter into a contract with all applicants. Or if the data subject does not want to provide such a consent, he/she has always the alternative of not entering the contract.[52]

From a different viewpoint, others may contend that almost no contract is consensual because there is always pressure for everyone, for one reason or another, in order to live in this world. This leaves no choices for the parties except to enter into contracts. This is the view expressed by Hale, who believed that people have no choice but to enter contracts for any aspect of their life so that 'coerciveness is not a ground for condemnation except when used in the sense of influence under pain of doing a morally unjustified act'.[53]

However, it seems that such views of the contractual type of consent neither correspond to the letter nor to the rationale of the provisions of the Directive, whose enactment finds its justification in the protection of the freedom of individuals and the other values explained earlier.

At any rate, these two views that share the thread to reduce the concept of consent to other concepts such as wrongdoing, efficiency, distributive justice and so on have been thoughtfully criticized on the ground that people do not make use of consent in either of the ways mentioned above and that the reasons for consenting

---

51 See, e.g., C. KUNER, *European Data Protection Law*, Oxford University Press, Oxford 2007, Ch. 5J; D. BAINBRIDGE, *Data Protection Law*, XPL, St Albans 2005; R. JAY, *Data Protection Law and Practice*, Thomson Sweet and Maxwell, London 2007, Chs 12 and 22.

52 See, e.g., P. ATIYAH, 'Economic Duress and the Overborne Will', 98.*The Law Quarterly Review* 1982, pp. 197–202; this view has also been explored by SMITH, *supra* n. 47, pp. 331–339.

53 R.L. HALE, 'Coercion and Distribution in a Supposedly Non-coercive State', 38(3).*Political Science Quarterly* 1923, pp. 470–494, at 476. See also F.A. HAYEK, *The Constitution of Liberty*, Routledge, London 1960. According to the author, for instance, 'even if the threat of starvation *(…)* impels me to accept a distasteful job at a very low wage, even if I am "at the mercy" of the only man willing to employ me, I am not coerced by him or anybody else' (p. 137).

are not the same as the consequences of consenting. In this latter sense, the difference that is emphasized is between 'consent' and 'causation'.[54]

Moreover, these are notions of consent that have been condemned for flirting with the myth of the equality of power in negotiations and relationships between organizations and individuals.[55]

Smith provides an interesting alternative account of consent. Focusing on the nature of the relevant pressure affecting the free and voluntary provision of consent in the context in which it is released, and accepting the imprecision of its notion, the scholar suggests that consent is free not only in the absence of pure states of necessity but also in the absence of substantively unfair contracts.[56]

This is also the view preferred by other scholars who robustly maintain that, for the notion of consent to work as a true source of personal responsibility, the individual would have to be in a strong bargaining position when facing a commercial organization.[57]

All these considerations have pushed consumer lawyers to the point of doubting whether there are any general principles of traditional contract law left where consumers are involved, stressing how in these circumstances contract law operates in a manner quite distinct from the classical notion of freedom of contract.[58]

Looking at the issue of consent from this perspective, it may be noted that the concept of 'unfair term' is employed in the language of European consumer legislation.[59] It finds its justification in the imbalance between supplier and consumer, as well as in the perceived need of the law to be shaped in accordance with the costs and benefits of having standard form contracts.[60] As such, the assessment of unfairness is subjected to the 'good faith' and 'significant imbalance test' in the parties, a notion that is also increasingly used in the area of data protection for the assessment of the provision of a valid consent by data subjects who are perceived to be in a position of having unequal bargaining power *vis-à-vis* data controllers.[61] Actually, some commentators stress that the rationale for the

---

54 SMITH, *supra* n. 47, pp. 332–333.

55 S. LEADER, 'Inflating Consent, Inflating Function, and Inserting Human Rights', in J. Dine & A. Fagan (eds), *Human Rights and Capitalism*, Edward Elgar, Cheltenham 2006, pp. 28–47.

56 SMITH, *supra* n. 47, pp. 331–339.

57 LEADER, *supra* n. 55, pp. 28–47.

58 See HOWELLS & WEATHERILL, *supra* n. 44, pp. 14–35.

59 Directive 93/13/EC, OJ 1993 L 95/29 replaced by Directive 2005/29/EC, OJ 2005 L 149/22.

60 HOWELLS & WEATHERILL, *supra* n. 44, Ch. 1.

61 Y. POULLET & J.M. DINANT, 'The Internet and Private Life in Europe: Risks and Aspirations', in A.T. Kenyon & M. Richardson (eds), *New Dimensions in Privacy Law*, Cambridge University Press, Cambridge 2006, pp. 60–90. T. LÉONARD, 'E-commerce et protection des données á caractère personnel: quelques considerations sur la licéité des pratiques nouvelles de marketing sur internet', *Internet & Recht*, Maklu, Antwerpen-Apeldoorn 2001, pp. 418–451; S. GARFINKEL,

data protection law in its current form is to enable individuals to bargain more effectively over the use of their personal information.[62]

Importantly, for the assessment of unfairness the tests make reference to the requirement of allowing a choice to the consumer, particularly in the absence of alternative contracts that do not contain the objectionable clause and clauses that make consent a condition of the contract. It is suggested that a standard industry practice for uses of information that effectively deprive the data subject of a choice is questionable where such uses are not essential for the purposes of the contract.[63]

Others further question the validity for data processing purposes of consumers' consent that is solicited in exchange for economic advantages or for fear of not being allowed to obtain goods or services or obtaining them of a lower quality.[64] This phenomenon is also known as 'engineered consent' or 'engineering of choice': if data subjects have to give more information than is strictly necessary to buy goods or access services then it is likely that they will consent to whatever broad uses of their data to obtain the goods or services they want. This objection has been supported by the Article 29 Working Party interpreting that 'consent given by a data subject who *(…)* has been presented with a *fait accompli* cannot be considered to be valid'.[65]

An area where such abuse of the data subject's consent has been so far identified is the labour market in the employer-employee relationship. This is due to the perceived inequality and disadvantage of employees in terms of bargaining power in the relationship and the resultant lack of proper consent in its 'freely

---

Database Nation, O'Reilly, Cambridge 2001, Chs 6 and 11; G. BUTTARELLI, *Banche dati e tutela della riservatezza: la privacy nella societa' dell'informazione*, Giuffre', Milano 1997, p. 285; Decision of the Italian Data Protection Authority, *Unione Italiana Bancari UIB/SBG* v. *Camera Sindacale Provinciale Asterisco di Bolzano* of 13 Feb. 1998; Decision of the Italian Data Protection Authority, *General Decision on 'Smart (RFDI) Tags: Safeguards Applying to their use*', 09 Mar. 2005; Y. POULLET, 'Making Data Subjects Aware of their Rights and Capable of Protecting Themselves', *Conference on the Rights and Responsibilities of Data Subjects organised by the Council of Europe and the Office for Personal Data Protection of the Czech Republic* (Prague, 14 and 15 Oct. 2004).

62 P.E. AGRE, 'Introduction', in P.E. Agre & M. Rotenberg (eds), *Technology and Privacy: The New Landscape*, MIT Press, Cambridge 1997, pp. 1–28, at 12.

63 See, e.g., JAY, *supra* n. 51, pp. 152–153; G. HOWELLS, 'Data Protection, Confidentiality, Unfair Contract Terms, Consumer Protection and Credit Reference Agencies', 4.*Journal of Business Law* 1995, pp. 343–359.

64 POULLET & DINANT, *supra* n. 61; LÉONARD, *supra* n. 61; DAVIS, *supra* n. 22, pp. 143–165; YOUNES-FELLOUS, Commission Nationale de l'Informatique et des Libertés, *Workshop on Privacy and Data Protection Issues* (Brussels 13 Feb. 2007). According to D. GIBSON, *Aspects of Privacy Law*, Butterworths, Toronto 1980, 'consent' clauses in application forms 'can hardly be regarded as voluntarily given, since the subject's free-will is likely to have been overborne by the desire to succeed in the application' (p. 122).

65 Article 29 Working Party on Data Protection, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114 of 25 Nov. 2005 for Adoption, 11.

given' element.[66] True, the example of the labour relation may not be entirely satisfactory for commercial transactions if one looks beyond an already established employer-employee relationship. In fact, it could be argued that the situation would be different when individuals are in the open job market. Here, it could be said, they will have a free choice whether or not to apply for a particular job. If consent to a certain processing of personal data is a condition of an application being considered, this would not prevent the consent being freely given. As the British Information Officer has stated, however, 'as recruitment proceeds the opportunities to obtain valid consent are likely to be reduced. If for example, the consequences of not consenting is the automatic withdrawal of a job offer the consent is unlikely to be given freely'.[67]

In the end, therefore, consent might be formally free in the sense that there is not a single or traditional method of forcing individuals into a transaction by commercial organizations, but if the costs of not consenting are considerable in relation to the situation at stake and there are no live options, then consent can be said not to be materially free.[68]

6.4. Specificity and the Other Requirements of the Law

Some may think that 'consent' may be sufficient to legitimize data processing on those occasions where no other legitimizing circumstances of the Directive are met. However, in the terms of the Directive and most of the national implementing legislation, consent does not exist in isolation. On its own, it does not appear to be a sufficient basis for legitimate data processing but must be considered in conjunction with other requirements, particularly those relating to specificity, purpose limitation, and proportionality.[69] For example, it would be a violation of the data protection principles to ask consumers to sign authorizations, unlimited in subject matter, essentially purporting to give permission to data controllers to process any personal data that they unilaterally decide to be relevant, and disclose that information for expanding purposes to any person willing to pay for it. By contrast, this study has already emphasized that one of the primary concerns of the Directive is to ensure that data subject's consent specifically to all uses for which the data is processed. A processing based on consent cannot be regarded as lawful if sought for general or vague aims or if the data subject has no possibility of knowing the

---

66 *Ibid*. R. FRAGALE FILHO & M. JEFFERY, 'Information Technology and Workers' Privacy: Notice and Consent', 23.*Comparative Labour Law and Policy Journal* 2002, pp. 551–567. See also CAREY, *supra* n. 39, pp. 72–73.

67 British Information Commissioner, available at <www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/supplementary_guidance/conditions_for_processing_sensitive_data.html>.

68 LEADER, *supra* n. 55; L. BECKER, *Property Rights: Philosophical Foundations*, Routledge, London 1977, pp. 76–77; AGRE, *supra* n. 62.

69 See, e.g., POULLET & DINANT, *supra* n. 61; KORFF, *supra* n. 35.

recipients of his/her data. This would be regarded as a way to evade the limitations imposed by the law.[70]

Moreover, since consent must be specific, it could be problematic to obtain the data subject's consent if the occurrence and specific circumstances of a processing are not known at the time consent is requested, so that the impact on the data subject cannot be assessed.[71]

In the implementation of the Directive, several countries have made it clear that even if a controller obtains the consent of the data subject, there are still the other requirements of the law to be respected, and a processing that does not meet those requirements is unlawful irrespective of the consent. This is because the right to data protection is often viewed not only as a personal right but also as a public concern and an issue of social protection embedded in the Constitutions of a number of Member States.[72]

6.5. Revocability of Consent

As a unilateral act, it is inherent in its nature that it can be withdrawn by the data subject at any time, albeit without retrospective effect.[73] Thus more, consent may be withdrawn if the data processing is not necessary for the service provided or it may be denied for a further processing that may be compatible, but still different, from the original purpose of the processing. This is also the reason why consent is seen as an unlikely and ephemeral mechanism to provide an adequate long-term framework for data controllers in cases of repeated communications and further processing.[74] Again, some may be tempted to think that a solution could lie in contract: consent, in fact, would not be withdrawn by a data subject, at least for a certain lapse of time, if it had been given under contractual arrangements that limit its withdrawal. However, for all the reasons explained above, in legal terms such an obligation should not be incorporated in the standard terms of a commercial agreement with consumers, leaving no option to consumers to exercise the right of withdrawal.

In the end, therefore, there remains little alternative but to agree with the Article 29 Working Party when it interprets consent in data protection in a restrictive manner, to the point of suggesting that 'relying on consent may therefore

---

70 Consent must be specific. Directive 95/46/EC, Art. 7(a).

71 See, for example, Art. 29 Working Party, *supra* n. 43.

72 See KORFF, *supra* n. 35, pp. 74–78; R. WONG, 'Privacy: Charting Its Developments and Prospects', in M. Klang & A. Murray (eds), *Human Rights in the Digital Age*, Cavendish, London 2005, pp. 147–161.

73 KORFF, *supra* n. 35, reports the UK Information Commissioner suggesting that 'even when consent has been given it will not necessarily endure forever. While in most cases consent will endure for as long as the processing to which it relates continues, data controllers should recognise that the individual may be able to withdraw their consent' (p 78).

74 Article 29 Data Protection Working Party, *supra* n. 43.

prove to be a "false good solution", simple at first glance but in reality complex and cumbersome'.[75]

PART III

7. Limiting Abuse, Confusion, or Conflation of Consent

Policy documents reveal that ensuring informed and free consent remains a priority for a comprehensive approach on personal data protection in the EU.[76] Likewise, Article 8 of the Charter of Fundamental Rights of the EU mandates the consent of data subjects as a core condition to enjoy the legal right to the protection of personal data in the EU.

However, it has been shown earlier how growing abuse, confusion or conflation of consent have made it unreliable to guarantee a high level of protection for data subjects, which makes it difficult its reconciliation with the policy objectives set at EU level.

The current normative approach to consent reflects the argument that the right to data protection rests on the individual's choice about the processing of his/her data and that no one is better placed to judge and decide about the use of data than the concerned data subject himself/herself. Such liberal conception of autonomy and approach based on individualism may be acceptable if supported by the liberal stance that personal information may be an alienable commodity in a proprietary sense to be protected or traded at the discretion of the individual to whom the information pertains. In any case, it would assume the absence of information asymmetry and power inequality between data controllers and data subjects. Equally, it would underestimate that secondary transfers and data mining make it almost impossible for ordinary people to verify in what measure the conditions for data processing have been respected. Besides, it would not consider the issue of positive discrimination: signalling by others may render the free choice of consent a façade to avoid the stigma attached to silence or not consenting for the processing of information. If a group of individuals finds it in his self-interest to disclose information for perceived benefits, others may need to disclose their personal data to avoid the stigma attached to silence or for not being present in a database (i.e., positive discrimination).[77] Finally, such approach would overlook

---

75 *Ibid*.

76 European Commission, *supra* n. 1.

77 On signalling and disclosure of personal information, see S.R. PEPPET, 'Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future', forthcoming in *Northwestern University Law Review* (2011), available on SSRN at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678634>.

that disclosed personal data may be relevant not only to the data subject but also to others with whom he/she entertains or has entertained relationships of any nature.[78]

This work has attempted to show that data protection is tied to substantial values for a democratic society. Thus, there may be a paradox or a conflict between the described current normative approach and all that has been said earlier in this work about the importance of data protection and the required high level of safeguards. For that reason, stand-alone normative solutions based on enhanced individual control and empowerment of data subjects seem unsatisfactory *vis-à-vis* the challenges posed by the complexities of business models, customer relationships, and technologies. Moreover, they would reinforce the assumption that the formal voluntary acceptance of data processing and disclosure causes no harm or problem precisely because it reflects the active choice of the concerned individual, meeting the formal requirement of the law.

Certainly individual control over information is important as long as the real meaning of consent is fully accepted and applied in practice. In this sense, it has to be agreed with the stance that the potential of the position of data subjects in Directive 95/46/EC has not been fully used and the new European legal framework should specify the requirement of consent to give *ex ante* a stronger voice to data subjects.[79]

Accepting that data protection is not only an individual right but also a social good with profound social implications, some scholarship has indeed recognized that protecting personal data rests not only on respect for individual autonomy but also on social welfare concerns, social freedom, and participatory democracy. Even this scholarship, however, concedes that data protection is not exclusively a social good, and individuals should retain the ability to exercise control over their information.[80]

It seems unquestionable that data protection is a tool to protect a free society where individuals freely develop their personality, that is, a social good. Nevertheless, there may be a degree of contradiction in continuing to assume and not departing from the proposition that individuals should remain able to alienate their personal data so long as they are fully informed and do it voluntarily. Or at least, the scholarship's response does not fully address solutions beyond individual control.

It is not suggested that the data protection regime should liberate from the constraints of consent and self-determination or abandon the stance that data protection should involve a degree of personal control over information. On the contrary, transparency and explicit true consent remain key to inform a properly

78 ROUVROY & POULLET, *supra* n. 20.

79 Articlee 29 Data Protection Working Party, *supra* n. 4.

80 See, e.g., SCHWARTZ, *supra* n. 48; D.J. SOLOVE, *Understanding Privacy*, Harvard University Press, Boston 2008.

functioning policy for the enhancement of individual autonomy and the full development of people's personality in a free society. However, to be effective, a better application of consent or specification of its requirements should be assisted with measures that go beyond the idea of individual control and autonomy.

A solution may rest on the correction of the limits of autonomy-enhancing measures with additional legal constraints that might prevent or reduce abuse, confusion, or conflation. Such legal constraints would not be any different from those that inform consumer law and policy. As in the consumer law domain, they could be explained on a number of different bases. This work has mentioned before of the power and information inequality between data controllers and data subjects, which would justify further regulation to correct a market failure. Equally, another ground for justifying such constraints could be found in the enhancement of distributive justice and ends, that is, in the redistribution of resources or rights on the basis of what is fair rather than what is merely economically efficient to protect data subjects as the weaker party of the data controller-data subject relationship.

Probably, however, paternalism would better explain additional legal measures that would find their justification in the social judgment that data protection is a tool to protect a social good and even if transacting free agents allow for the processing of their data over certain permitted levels, which should be prohibited because of social harm is greater than the benefits of allocative efficiency typical of freedom of contract.

Libertarians may argue that such interfering with individual autonomy and free choice is not a marginal cost. Anglo-Saxon scholarship and liberal ideology, in particular, could be wary to accept overriding decisions by law-makers over individual autonomy and liberty.

An approach based on soft paternalism, however, would not necessarily deprive individuals from freedom of choice but only shove them towards wise decisions in the interest of society as a whole that are not simply taken to gain pressing illusory personal benefits of the moment. Soft paternalism or 'libertarian paternalism' indeed suggests that, while people remain free to choose, at the same time they are provided with cognitive escorts leading them towards the desired outcome for the welfare of society as a whole (and, ultimately, for their own welfare).[81]

This approach would involve legislation adopting, as a default rule, an outcome that is desirable to protect the social good in the interest of society but where individuals might opt-out for an alternative, less desirable outcome. Thus, alongside the existing rules that restrict the use that data controllers may do with personal data irrespective of the way they have obtained them, there should be

81 On soft legal paternalism see, e.g., A. OGUS, 'The Paradoxes of Legal paternalIsm and How to Resolve Them', 30.*Legal Studies* 2010, pp. 61–73; C. SUSTAIN & R. THALER, 'Libertarian Paternalism Is Not an Oxymoron', 70.*The University of Chicago Law Review* 2003, pp. 1159–1202.

complementing measures normatively addressing inquiry (from data controllers) and disclosure (from data subjects) boundaries to reinforce informed explicit consent.[82]

Inquiry limits are rules that restrict the ability of an uninformed party to ask for disclosure from the party who has the information. At the same time, they should be accompanied by normative directions as to the bar over attaching negative consequences for silence or failure to consent to data processing. For example, this already exists in the case of legislation forbidding potential employers from asking a potential employee his/her age. In the data protection realm, thus, alongside informed explicit consent it would be a matter of normatively introducing as a default rule that data controllers may not seek data processing permissions in one instance specifying that more instances of consent depending on strict processing purposes should be sought without affecting the capability of data subjects to obtain the goods or services they apply for.

A possible example may be that of the Canadian Personal Information Protection and Electronic Documents Act 2000, which contains an explicit 'refusal to deal provision', prohibiting organizations from requiring consent to unnecessary processing as a condition of the transaction, demanding additional consent for it.[83]

Equally, to remove psychological barriers to provide consent, the law should contain comprehensive normative disclosure limits, making it explicit that data subjects may always be allowed to refuse consent or withdraw it at a later stage without negative consequences or strings attached.

Finally, normative qualification would be needed that data processing consent is a unilateral act that cannot be part of the agreement of the general terms and conditions of contract for those data that are not strictly necessary for the provision of a service or supply of goods: data subjects' consent would be invalid when incorporated in a commercial contract if the data subject cannot express consent separately from his/her consent to contract. Take the example of fidelity cards used by supermarkets: it would be perfectly legitimate to offer such cards to customers to make them loyal, offering prizes or discounts once a certain accumulation of points has been reached. The data processing would be required for the purpose of running the scheme and the benefit for the data controller would be the loyalty of customers. However, there should be no contextual processing for profiling customers or further disseminating their data. Even better, customers should be asked in a separate instance of consent whether they wish this to happen knowing that no consequences would be attached for their refusal and that nevertheless they would enjoy the same level of discounts or prizes.

---

82 Also referred as 'don't ask' and 'don't tell' rules. See PEPPET, *supra* n. 77.

83 PIPEDA Sch. I, Principle 4.3.1 (n. 37). See P. LAWSON & M. O'DONOGHUE, 'Approaches to Consent in Canadian Data Protection Law', in I. Kerr *et al.* (eds), *Lessons from the Identity Trail*, Oxford University Press, Oxford 2009, pp. 23–42.

In the end, a form of legislative intervention grounded in soft paternalism may be consistent with traditional notions of individual autonomy where there would be no requirement with which individuals would be forced to comply with. Rather, it would be a question of the extent to which such device is effective in pushing, not forcing, individuals towards the desirable outcome for society as a whole.

Some may reasonably say that Directive 95/46/EC already requires data minimization and purpose specification. However, given the current practices and data mining techniques, the letter of the law should leave no doubt and it should not be left open to different interpretations. At any rate, the real innovation or strengthening of the rules of consent envisaged by EU policy makers would insist in the choice to data subjects of opting out to added default rules aimed at impeding those very technological and commercial practices that have driven the need for modernization of the existing EU regime.

8. Theoretical Model for Additional Legal Constraints

Although legal paternalism is well rooted in the European heritage and there may be a greater readiness to recognize that the State should take responsibility to promote social welfare and protect his weaker members,[84] there may be difficulties for policy makers with a solution that would almost certainly override economic interests. As for privacy, the perception of the harm caused by the weaknesses of the data protection regime, generally, and the current form of consent, in particular, remain abstract, and the threats posed by data processing abuses may be easily often perceived as intangible. As a consequence, such intangible harm and risks may not be concrete enough to induce legislators to take action *vis-à-vis* the prospect of data controllers better marketing products to consumers or more accurately assessing credit risks or *vis-à-vis* the powerful lobbies of the data controllers.[85]

Crucially, however, the Treaty of Lisbon has tightened data protection and mandates a stricter regime where data protection may not be seen any longer as a purely 'functional construct to be used to directly shape and influence the use of information-processing technology'.[86] The European legislation has taken a holistic perspective where the declared key objective is the strengthening of individuals' rights *vis-à-vis* the more powerful data controllers. It derives its normative power from primary sources such as a 'provision of general application' of the Treaty of Lisbon (Article 16 TFEU) and the EU Charter of Fundamental Rights. Probably, from a legal positivist point of view, giving application to primary legal sources would be already a sufficient ground to override conflicting economic interests and

84 OGUS, *supra* n. 81, pp. 65–67.

85 This is also a consideration made by PEPPET, *supra* n. 77, in the context of a signalling economy and the digital dossier.

86 MAYER-SCHONBERGER, *supra* n. 17, p. 235.

rebalance the participatory self-determination of data subjects in the information market.

Therefore, it may be maintained that in the new framework the increased profits of the industry may not of itself warrant the same lax practices of obtaining data subjects' consent and stricter rules on consent may be tolerated. On the contrary, perhaps, the EU legislator may be persuaded to sacrifice such aspect of the right to data protection in the interest of the economic benefit of society generally. Such utilitarian arguments, however, would need to be very strong in order to outweigh the effective protection of a fundamental right enshrined in the highest ranks of EU law. So, any possible utilitarian argument would be justifiable only if one takes an 'interest' perspective out of the notion of data protection. This perspective would see the protection of personal data as one among many interests in society, including the commercial exploitation of personal information. Responding to the above utilitarian view, these 'interests' would need to be balanced in the light of overall social utility.[87] As the situation stands, however, data protection is a legal right. The 'right' perspective embedded in European legal culture, however, should give its preferred position at least against those interests that are not characterized as legal 'rights'. After all, as rightfully pointed out by others, 'in Europe, there is a politico-legal commitment to respect for human rights; that is *(…)* Europe has chosen rights rather than utility as the governing ethic'.[88] Thus, data protection as a legal 'right' with derivation from European law should trump interests such as the commercial exploitation of personal data.

Common law lawyers would probably be more comfortable with the theoretical position encapsulated in Ronald Dworkin's notion of 'rights as trumps' to accord a higher justificatory status to data protection rights than the economic advantages resulting from the commercial exploitation of personal data by data controllers. Within this theoretical model, rights are to be protected and promoted to the greatest extent possible before other interests could be taken into consideration. However, common law lawyers may encounter some difficulties in the defence of this position to the extent that Dworkin concedes that rights may legitimately be limited where the cost to society would be of a degree far beyond the price paid to grant the original right,[89] which in some commentators' view 'amounts to saying that rights are not conclusive, but only create strong presumptions that

87 See also HOWELLS, *supra* n. 63, pp. 353–354.

88 BROWNSWORD, *supra* n. 3, p. 85.

89 See R. DWORKIN, *Taking Rights Seriously*, Duckworth, London 1977. In the author's famous formulation, rights 'trump' utilitarian values.

the individual interests or choices at stake should be protected against collective encroachment'.[90]

Whatever the right-based theoretical model and approach are, this would justify and require commercial data controllers to find alternative methods for their aim or to accept making fewer profits – which would not mean making a loss but just accepting lower returns. Arguably, markets may be competitive without excessive profits being made. In fact, to what extent excess profits are optimal from the point of view of consumer welfare is a complex economic matter and remains open for discussion.[91]

By contrast, the increased awareness and recognition of the importance of data protection should not lead to what has been defined as a 'schizophrenia' where, on the one hand, it is reflected in the legal protection at the highest levels of EU law and policy but where, on the other hand, it is eroded by market interests that head towards the diminution, abuse, confusion, or conflation of the aspired safeguards or guarantees.[92]

9. Conclusions

This work investigated data processing consent as the linchpin of EU data protection legislation in light of the innovations of the Lisbon Treaty and the announced reforms of its legal regime.

At EU level, the recognition of data protection as a legal right dates back to Directive 95/46/EC. To meet the challenges of rapid technological developments and of the modern economy, the EU is undergoing consultations to reform the current legal framework and propose a new comprehensive regime. The TFEU and the Charter of Fundamental Rights of the EU have given new emphasis and significance to the protection of personal data, which is now a sui generis right clearly distinguished from privacy. Data protection has now been upgraded as a treaty provision of general application and formally recognized as a fundamental right of the EU. Indeed, data protection and privacy may be re-conceptualized as a bundle of legal rights and tools to pursue the common goal of a democratic society not only free from unjustified intrusion and surveillance but where citizens may develop their personality freely and autonomously through individual reflexive and active participation in society. Therefore, data protection principles, as a legal tool, should be seen as less procedural and more substantive to protect and guarantee the underlying fundamental values.

---

90 A. MCHARG, 'Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights', 62.*The Modern Law Review* 1999, pp. 671–696, at 683.

91 See I. RAMSAY, *Consumer Law and Policy*, Hart Oxford 2007, pp. 76–78.

92 S. RODOTA', 'Data Protection as a Fundamental Right', in S. Gutwirth *et al.* (eds), *Reinventing Data Protection?*, Springer, Heidelberg 2009, pp. 77–82.

Data processing consent is a crucial component of data protection law to give effect to the goal it purports to achieve. Reflecting a classical liberal conception of autonomy and individualism, in which individuals ought to know what is best for themselves and are able to take decisions accordingly, it provides individuals with some control over their personal information and the persona they project in society. However, the way in which it is currently devised in the law and its application provide an insufficient protection for individuals and an inadequate safeguard for the values it aims to protect *vis-à-vis* the realities of marketplace practices and economic interests.

There is certainly some truth in the opinion of the EU data protection authorities that the full potential of the position of data subjects in the law has not been fully exploited and the current data protection principles remain valid. This work has analysed the meaning of a real consent to inform a better application of its notion against possible confusion, conflation, or abuse. At the same time, however, taking into account the inherent weaknesses of consent as a safeguard of a social good, additional legal measures would be necessary for a better application and specification of the requirements of consent. Additional norms to be introduced in a new data protection regime should adopt, as a default rule, an outcome that is desirable for society as a whole but where individuals might opt-out for a different outcome without gains at the expense of the goals that the law aims to achieve – or specifying that refusal to consent or silence should not bear negative consequences for the underlying transaction. The suggestion is that there should be inquiry and disclosure limits complemented by the normative qualification of consent as a unilateral act, with all the following legal consequences that this entails. This work has addressed a possible solution in soft or libertarian paternalism to compromise between traditional views of individual autonomy and the need to raise the safeguards for an effective self-determination for the extent made possible by the law. After all, a liberal democracy that embraces values of citizen participation and autonomy should take rights seriously and lead not only to a greater but also to an effective control by citizens over their information.

Admittedly, policy makers may find difficulties in resisting or overriding strong economic interests in the absence of tangible harm or threats. However, a rights-led approach as it is now imposed by the Treaty of Lisbon and the EU Charter of Fundamental Rights, supported by a legal positivist theoretical model, means that data protection cannot remain an empty box and should override economic interests. The notion of consent should not be fictionalized, which occurs when the formal quality of consent is conflated or confused to cover and abuse unequal power relations beyond the state.[93] Each legal regime has certain fundamental value commitments, in these cases the protection of dignity, liberty,

93 LEADER, *supra* n. 55.

participation, and data protection. Thus, as rightly reminded by Beyleveld and Brownsword, 'to the extent that a legal regime claims legitimacy for its operations, it claims, first, that its operations are consonant with such basic constitutional values and, secondly, that these values themselves are worthy of respect (as legitimate)'.[94]

To the extent that legal regimes owe a duty to maintain public confidence in their operations and respect for the constitutional values and regulatory positions that they take, such as data protection, consent should be taken seriously and its procedural justification should not abused; otherwise, it would become unclear whether the legal regime operates legitimately.[95]

94 BEYLEVELD & BROWNSWORD, *surpa* n. 31, p. 358.

95 *Ibid*.

EUROPEAN REVIEW OF PRIVATE LAW
REVUE EUROPÉENNE DE DROIT PRIVÉ
EUROPÄISCHE ZEITSCHRIFT FÜR PRIVATRECHT

Guidelines for authors

The European Review of Private Law aims to provide a forum which facilitates the development of European Private Law. It publishes work of interest to academics and practitioners across European boundaries. Comparative work in any field of private law is welcomed. The journal deals especially with comparative case law. Work focusing on one jurisdiction alone is accepted, provided it has a strong cross-border interest.
The Review requires the submission of manuscripts by e-mail attachment, preferably in Word. Please do not forget to add your complete mailing address, telephone number, fax number and/or e-mail address when you submit your manuscript.
Manuscripts should be written in standard English, French or German.

Directives pour les Auteurs

La Revue européenne de droit privé a pour objectif de faciliter, par la constitution d'un forum, la mise au point d'un Droit Privé Européen. Elle publie des articles susceptibles d'intéresser aussi bien l'universitaire que le praticien, sur un plan européen. Nous serons heureux d'ouvrir nos pages aux travaux comparatifs dans tout domaine du droit privé. La Revue est consacrée en particulier á l'étude comparée de la jurisprudence. Les travaux concentrés sur une seule juridiction sont admissibles, à condition de présenter un intérêt dépassant les frontières.
Nous souhaitons recevoir les textes par courrier électronique, de préférence en Word. Ajoutez l'adresse postale compléte et le numéro de téléphone de l'auteur, un numéro de télécopie et l'adresse électronique.
Les textes doivent être rédigés en langue anglaise, française ou allemande standard.

Leitfaden für Autoren

Die Europäische Zeitschrift für Privatrecht will ein Forum bieten, um die Entwicklung des europäischen Zivilrechts zu fördern. Sie veröffentlicht Arbeiten, die für Akademiker und Juristen in ganz Europa grenzüberschreitend von Interesse sind. Vergleichende Untersuchungen aus jedem Bereich des Zivilrechts sind willkommen. Die Zeitschrift befasst sich insbesondere mit vergleichender Rechtsprechung. Artikel, die sich auf ein einziges Hoheitsgebiet konzentrieren, können angenommen werden, wenn sie von besonderem grenzüberschreitenden Interesse sind.
Wir möchten ihre Beiträge per E-Mail erhalten und bevorzugen Dateien in Word. Bitte geben Sie ihre Anschrift, Telefonnummer, Telefaxnummer und/oder E-Mailadresse an.
Manuskripte sind in korrektem Englisch, Französisch oder Deutsch zu verfassen.

Style guide

A style guide for contributors can be found in volume 19, issue No. 1 (2011), pages 155–160, and online at http://www.kluwerlawonline.com/europeanreviewofprivatelaw.

Index

An annual index will be published in issue No. 6 of each volume.