Privacy and the regulation of 2012

Poullet, Yves; Gaspar Costa, Luiz

Published in:
Computer Law and Security Review

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Privacy and the regulation of 2012

Luiz Costa, Yves Poullet

CRIDS, University of Namur, Belgium

Keywords:
General data protection regulation
Data protection
Personal data
Privacy
Right to be forgotten
Supervisory authority
Data protection by default
Data protection by design
Data protection impact assessment

ABSTRACT

This paper explores the European Commission's proposal for a new Regulation to update and reform data protection law in Europe. As regards the Regulation itself, without presenting an exhaustive analysis of all the provisions, this paper aims to highlight some significant changes proposed to the data protection regime by comparison between Directive 95/46 and the proposed Regulation. It takes particularly into account legislative innovation concerning data protection principles, data subjects' rights, data controllers and data processors obligations, and the regulation of technologies. Before analyzing these innovations, it introduces some considerations about the Commission's choice to use a Regulation instead of a Directive to harmonize national data protection regime.

1. Introduction

On 25 January 2012 the European Commission presented the proposal for a Regulation on the protection of individuals with regards to the processing of personal data and on the free movement of such data; the so-called "General Data Protection Regulation"[1] (cited herein after as "the Regulation"). When it comes into force, the document will be the new general legal framework of data protection, repealing Directive 95/46 more than twenty-seven years after its adoption. At the same time and constituting what is the "Data Protection Package", the Commission introduces a proposal for a Directive on the protection of individuals with regards to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.[2] This second text will not be commented in the present article.

2. Regulation instead of directive

The harmonization obtained by the Directive 95/46 has seemed insufficient. The strong reassertion of the Data Protection as a fundamental right, both by the article 8 (1) of the 2000 EU Charter of fundamental rights and by the article 16 (1) of the Treaty, requires an effective and more coherent protection of the EU citizens throughout the European Union. It might be added that due to the increasing number of data flows and their globalization, Europe might no longer accept different national data protection legislations both as regards their content and their effectiveness. That situation hampers the functioning of the internal market and co-operation between public authorities in relation to EU policies, creates confusion and uncertainties for data controllers and provokes a loss of trust for citizens. Furthermore, this lack of full harmonization weakens the capacity of EU to speak with one voice at the international level. That is why,

[1] COM(2012) 11 final. A first version of the draft has circulated, dated from 29/11/2011. The final draft introduces certain minor modifications.

[2] It means that the Regulation is not applicable to the processing activities related to these purposes and subject to this specific Directive. This decision seems in contradiction with the suppression of the traditional pillars and might create certain uncertainties as regards the precise scope of the two texts.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2012.03.015

in order to ensure a full consistent and high level of protection equivalent in all the EU member states, a Regulation was judged as the adequate solution to ensure full harmonization.

That solution has different consequences. First, the text adds to the powers of the Commission to define and implement certain provisions[3] or to adopt specific texts as regards certain sectors. The exercise of these delegations is under the sole control of the EU Parliament and Council. Secondly, as we will develop later, the text provides a stronger uniformity as regards the quality, the competence and the powers of the national Data Protection Authorities (DPA) (Chapter VI, art. 46 and ff.), reinforces their co-operation (Chapter VII, Section 1) and puts into place a "consistency mechanism", which obliges each DPA to cooperate with each other and with the Commission. Thirdly, the Commission through different mechanisms of notification and evocation will monitor the different decisions taken by the Member States.

3. Less privacy, more data protection?

Both Directive 95/46 and the Regulation present data protection and free movement of personal data as their objects. Nevertheless, it is worth noting that Article 1 of Directive 95/46 provides that Member States must "protect the fundamental rights and freedoms of natural persons and **in particular their right to privacy** with respect to the processing of personal data". Instead, Article 1, 2, of the Regulation previews among its objectives the need to "protect the fundamental rights and freedoms of natural persons and **in particular their right to the protection of personal data**". The Regulation clearly dissociates data protection from privacy and launches its basis exclusively on the first one; the word 'privacy' is gone. In addition, the distinction is reinforced when the Regulation establishes the concepts of "data protection assessment" and "data protection by design", which are clearly unusual terms in comparison with "privacy impact assessment" and "privacy by design". The word 'Privacy' appears 13 times in Directive 95/46 while only three times in the Regulation. Is data protection breaking up with its origins? If yes, what will be the outcomes of this movement? New legal correlations between privacy and data protection must be established? The outcomes of this change are still to come, but it is certain that affirming the autonomy of the right to the protection of personal data does not imply denying privacy as its fundament. That distinction puts protection of liberties at risk since it cuts the Data Protection regulation from the innovative and quite protective Strasbourg Court's jurisprudence which repeats that privacy might be considered as the way to achieve the right to self-determination, to dignity and, to that extent, represents an essential condition for all liberties. One must reassert the intrinsic link between Privacy and Data Protection legislation that, in an information society, is viewed as a simple tool for conserving the different human liberties rather than as an end *per se*.

[3] See the long list enumerated in Article 86.

4. Which personal data?

Under Directive 95/46 the concept of personal data is related to nominative identification. According to Article 2, a, personal data is:

> *any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*

Technological innovations have called this concept into question. 'Identifiability' implies distinguishing someone among others, notwithstanding the knowledge or the potential knowledge of his or her names. Traditionally personal data means potential reference to nominative data, within private and public IT systems, e.g. the public registration number, names, addresses, health and financial data. However, today, the use of certain technologies allows contacting and even profiling people regardless of any nominative information. In other words, data processors do not even need to know who is the data subject behind such data in order to make him or her identifiable; for instance, it is enough to know his or her navigation habits through a cookie or an Internet protocol number, or his or her movements through a tag linked with an object in his or her possession. This means that it is possible to process particular, peculiar data about a person without the need to reveal his or her nominative identity. Since the concept of personal data in Directive 95/46 was unclear and was considered usually as not taking these possibilities into account[4], a loophole existed that placed privacy at risk.

This risk is not disregarded by the Regulation, which states in the Preamble that:

> *when using online services, individuals are associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. Since this leave traces which, combined with unique identifiers and other information received by the servers, can be used to create profiles of the individuals and identify them, this Regulation should be applicable to processing involving such data.*

According to the Regulation, personal data is any information relating to a data subject and data subject is

> *an identified natural person or a natural person who can be identified, directly or indirectly,* ***by means reasonably likely to be used by the controller or by any other natural or legal person****, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person* [emphasis added] (Article 4,1).

[4] See however the opinion of the Art. 29 WG, Working Paper 4/2007 on the concept of personal data, WP n° 136 (June 20, 2007) which aims to enlarge the concept of personal data, taking into account that a processing might affect an individual which as such is not identified and will never be identified by his or her name.

What interpretation is released from the Article here, especially from the reference to the means reasonably likely to be used to identify a person? Assuming that the novelty in the wording is intended to offer more protection to citizens, we can speculate that 'identifiability' implies a need for data protection, regardless of the used means. These means are presumably nominative data, terminal identifiers or any other identifier because, if someone can be distinguished from other people, data protection legislation is applicable. If this is correct, one could say that the Regulation is more protective than the Directive since it clarifies situations where legislation is incidental. One aspect of privacy and data protection is a remedy against intrusiveness and loss of control of the circulation of a person's informational image. Such intrusiveness and its loss do not only exist when someone is or can be identified; for instance, the acts of being observed and being traced are privacy threats, even without knowing the name of the observed or traced person.

5. Transparency

Relations between citizens, governments and industry are asymmetric and data protection legislation faces the challenge to protect citizens, counterbalancing the strength of governments and industry. The asymmetric knowledge about the functioning of IT is one source of this imbalance of strength. Citizens are rarely aware about how their data are collected and processed while they are surfing on the Internet at home, using their cellphones, walking down a video-surveyed street or with an RFID tag embedded in their clothes and so on. In this context, transparency is a normative value that talks about being open and clear and is a remedy against obscurity and opacity: in relation to data processing, transparency translates the widening of the knowledge about information systems. If transparency was considered, from the very first texts, to be a major principle of the general data protection framework, it was at first coupled with the principle of fairness.

According to the previous texts, Article 5, a, of the Regulation stipulates that personal data must be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*". Furthermore, transparency requires greater awareness among citizens about the processing going on: its existence, its content and the flows generated in and out by using terminals. This means that it is present not only in the statement of its substance and procedures (Articles 11, 12 and 13) but also in every rule related to its core. For instance, providing information is an essential way to make transparency effective. To do this, one must know both what and how to make information available. Therefore, rights concerned with information and access to data (Articles 14 and 15) are clearly related to transparency. But these deductions are classic and not very innovative. In our opinion, the authors of the Regulation have not been sufficiently innovative, for the greater the flow of information the more opaque it becomes in modern information systems and with new ICT applications. In that case the right to transparency must increase alongside these new processes.

It is worth noting that, as in the Directive, the Regulation establishes a minimal list of information to be provided to citizens ("*the controller shall provide the data subject with* ***at least*** *the following information* […]"). It would have been interesting to have given data controllers new specific duties. Does transparency imply that the controller must provide specific information where more complex infrastructure is involved – for instance information about how tags and readers work in RFID applications – even though not previewed in the Regulation? If yes, what standards should operate to guide the provision of information? As regards the use of profiling systems, should it be necessary to give information about the logic between the building-up of the profiles. New transparency duties could also operate among terminal producers in order to ensure that the functioning of these terminals will be transparent for his or her user.

Transparency is also related to data security and risk management. Evaluating risks is a motto constantly repeated in our societies, and in the Regulation the communications of personal data breaches to the subject and data protection assessment are two examples of this risk approach. In relation to the first one, we know that according to the Data Protection principle, data controllers and processors must take measures to assure a level of security appropriate to the risks to personal data. That assertion is already present in the Directive. The Regulation will lay down the consequence of insufficient security by regulating the personal data breach in a largely more extensive way than that enacted in 2009 in the e-Privacy Directive concerning certain telecommunication operators' processing. So a personal data breach is the causation of "accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Article 4,9). In this context, when a personal data breach occurs the controller must notify the supervisory authority (Article 31) and communicate with data subjects if there is risk of harm to privacy or personal data (Article 32).

What outcomes then are to be expected from the arrival of the transparency principle in data protection legislation? How will it interact with other data protection principles? By means of enhancing awareness about risk, does transparency engender a general "right to know" among individuals?

6. Control-rights: the right to be forgotten and the right to data portability

People have very limited control over their personal data, which are more and more processed and archived indefinitely. The common ground between the right to be forgotten and data portability is found in the objective to strengthen data subjects' rights since both grant prerogatives through which persons can affect the processing of their personal data.

6.1. *Right to be forgotten*

The Regulation establishes the right to be forgotten and to erasure, which consists of securing from the controller the erasure of personal data as well prevention of any further dissemination of this data. In this context we will now glimpse at its fundaments, the relations between this right and traditional data protection principles and rules as well as perspectives on its effectiveness.

The right to informational self-determination lies at the root of the right to be forgotten. Based on the fundamental principles of dignity and self-development, the right to informational self-determination "*provides individuals the power to decide themselves about issues of collection, disclosure and use of their personal data*".[5] The Regulation states that the right to be forgotten has special relevance when the individual made data available while as a child. Here, a "clean slate" approach seems to be taken into account, the principle being that the right should relate to a protection against the negative use of past information.[6] The use of data from social networks in employment contexts is a representative example. Personal data such as photos taken in private contexts have been used to refuse job positions and fire people. But forgetfulness is larger. It is one dimension of how people deal with their own history, being related not only to leaving the past behind but also to living in the present without the threat of a kind of 'Miranda' warning, where whatever you say can be used against you in the future. In this sense the right to be forgotten is closely related to entitlements of dignity and self-development. Once again, privacy appears as the pre-requisite of our liberties, assuring the possibility to freely express ourselves and move freely on the street….

The right to be forgotten finds root in four instances in which its attributes are clearly related to some DP principles: where data are no longer necessary in relation to the purposes for which they were collected or processed (which recalls the finality principle); where data subjects have withdrawn their consent for processing; where data subjects object to the processing of personal data concerning them or where the processing of personal data does not comply with the Regulation – these last two hypotheses evoke the rights to rectify, erase and block data processing previewed within Article 12,b of the Directive 95/46. Beyond these general relations, the right to be forgotten amplifies the effectiveness of data protection principles and rules. For instance, while the Directive allows people to erase data only where there is no compliance with the law, the Regulation also grants individuals the right to erase where they have withdrawn their consent, which represents a clear increment to user control.

As elsewhere, the effectiveness of any right relies on the accountability of obligations established to a responsible reviewer. Three sorts of duties are established to the data controller: erasing data under his control and not processing them further; informing third parties that the data subject requests the erasure of data; and being responsible for publications done by third parties under his authorization (Article 17,2 and 8). The welcome statement of obligations clearly deserves further development. One issue, for example, is how to enforce the right to be forgotten where there is no direct relation between the subject and the data controller – e.g. a data mining company? Informing third parties of the individual's request to erase or block data can help to make the measures effective, but how do the rules constrain third parties to comply with a duty that was originally imposed only on the data controller? Since privacy is relational, how should they resolve conflicts between individuals – for instance, erasing common photos and posts on a social network website – when two persons oppose each other? Should the controller be the referee to evaluate a conflict between privacy and freedom of expression (Article 17,3)? If yes, which parameters should guide the controller?

The effectiveness of the right to be forgotten must also rely on a techno-legal approach. Which technical solutions should be adopted to assure the erasure and blocking data on Internet servers? How can these be made effective concerning data stored on terminal equipment such as computers and mobile devices? Answering these questions demand the establishment of "privacy-by-design" obligations. The creation of these obligations will depend on how the Commission specifies the conditions, criteria and requirements to (a) specific sectors and data processing situations, (b) the deletion of links copies and replications of personal data and (c) the restrictions to process data (Article 18,9).

6.2. *Data portability*

According to the Regulation, data portability is twofold. First, it implies the right of data subjects to obtain from the controller a copy of their personal data in a structured and commonly used format (Article 18,1). In this context, data portability is a kind of right to backup and use personal information under the management of the data controller. Second, data portability grants the right to transmit personal data and other information provided by the data subject from one automated processing system to another one (Article 18,2). Here, data portability is therefore the right to take personal data and leave.

The benefits of data portability are clear. As within the case of the Universal Service Directive's number portability, data portability empowers subjects as it liberates them from the constraint of having their data tied to a specific service provider. From this point of view, data portability gives more freedom of choice to people while at the same time stimulating competition among service providers. However, further developments are necessary to protect privacy. For instance, moving personal photos from a social network to another location may affect the interests of other individuals; what legal and technical solutions must be adopted to protect third party's privacy in this situation? What rules need to exist to balance conflicts between individuals?

7. Old principles, new dimensions?

The Regulation has changed the phrasing of the principles relating to adequacy, relevancy, minimization and consent.

A better choice of words is noted with regard to the amount of data to be processed. Directive 95/46 says data must not be excessive while the Regulation says it must be limited to the

[5] A. ROUVROY and Y. POULLET, "The right to informational self-determination and the value of self-development – Reassessing the importance of privacy for democracy", in *Reinventing data protection*, Proceedings of the Colloquium held at Brussels, Nov 2007, Springer Verlag, 2009. P. 56.

[6] A. ROUVROY, «Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?», in *La sécurité de l'individu numérisé. Réflexions prospectives et internationales.*, 2008, pp. 249–278.

minimum. In contrast, the second part of Article 5, c is not as clearly encouraging as the first one is. Let us highlight the concerned Articles from both texts, where personal data must be:

> *adequate, relevant and not excessive in relation to* ***the purposes for which they are collected and/or further processed*** in the Directive 95/46 (Article 6, 1, c)and

> *adequate, relevant, and limited to the minimum necessary in relation to* ***the purposes for which they are processed*** *[…]* in the Regulation (Article 5, c).

Data collection is essential because it is not only the entrance door of information systems, but also the very first act that places a person (i.e. her data) in touch with IT systems. Consequently, legislation surrounds data collection with special care, as when it establishes obligations upon the controller to provide quality information to the data subject even before the collection takes place. Another example is the Article 6, 1, c of Directive 95/46, which links the characteristics of adequacy, relevancy and non-excessiveness to the purposes of collection and processing of data. This means that these characteristics must be considered with regard to data collection; in other words, data collection circumstances – the moment it occurs and how it occurs for instance – are especially significant to define the legitimacy of data processing. In that context, it is a matter of regret that nothing has been said about the right of citizens to remain anonymous, each time an individual's identification is not necessary. We know that, for different reasons, most data controllers impose *a priori* the revealing of the names and other attributes of their potential customers even when no transaction or other justification makes that revelation pertinent.

Another point needs to be mentioned here. The Regulation cuts out the reference to the purposes for which data "are collected", in spite of maintaining mention of the purposes for which data "are processed". This might be understandable since collection is as such a processing. However, having suppressed the specific mention to the link between the collection of data on the one hand and adequacy, relevancy and minimum data on the other, the Regulation creates the risk that it might weaken the protection as regards the collection of data. With this open door, one could argue that the legitimacy of data processing does not particularly need to rely on the purposes established at the moment of collection.

At last, the consent framework is going to be significantly modified by the Regulation, which gives broader definition and conditions of consent compared to Directive 95/46. According to the Regulation, consent is any "freely given specific, informed and explicit indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed" (Article 4,8). The reference to "freely given, informed and explicit" attributes is clearer than the precedent "unambiguously" consent. However, the concept of the Regulation creates an odd reference to the "wishes" through which the data subject "signifies" the agreement to data processing. A wish is a desire and it is clear that people wish, desire to access new services, to amplify their experience with new technologies and applications and so on. Nevertheless, a wish is not synonym of will, which is a deliberate choice that produces legal consequences. Wishing to use a service is not a synonym to awareness of the legal consequences of saying yes specifically as regards the processing of personal data generated by this use. Will, rather than wishes, is at the heart of a data protection regime. Still further about the consent, the Regulation in its Article 7 establishes welcome procedural and substantive conditions. We highlight Article 7,4, which embraces the proportionality principle approach when it establishes that "consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller".

8. The framing of profiling

The classical protection in respect of automated individual decisions of the Directive (Article 15) is considerably enlarged in relation to profiling (art. 20 of the Regulation), which covers also the use of data correlations to predict behaviors or to take decisions vis-à-vis targeted people (e.g. citizens suspected of potential fiscal fraud). Doing so, the European Commission follows a recent recommendation of the Council of Europe regarding profiling (Nov. 25, 2010).[7]

Three points deserve special attention since they distinguish between the traditional regimes of automated individual decisions from the new one about profiling. Classical automated individual decisions take into account directly data referred to a certain individual in order to apply to these data automated reasoning. However, modern techniques of profiling are using huge nominate or innominate data (e.g. the average incomes of people living in a certain area) to define abstract profiles (e.g. people engaging in that kind of surfing at 85% are likely to be interested in those kinds of specific products or services or might be suspected of fiscal fraud). The profile is applied to a specific person known or unknown only as a second step, sometimes to take decisions or simply to gain better knowledge of the individual, notably in case of marketing. The Council of Europe defines profiling as "*an automatic data processing technique that consists of applying a "profile"* to an individual, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes".

The second point concerns the shift from the protection in regard to automated decisions (Directive 95/46) to the protection in relation to profiling (Regulation). Instead of

[7] In the context of the works done by the Council of Europe about profiling and privacy, J.M. DINANT, C. LAZARO, Y. POULLET, A. ROUVROY, "*Profiling and data protection*", Report addressed to the Convention 108 consultative Committee, September 2008, available on the Council of Europe website. See in the same sense, M. HILDEBRANDT, " Profiling and the Identity of the European Citizen", in *Safeguards in a World of Ambient Intelligence*, in WRIGHT David, GUTWIRTH SERGE, FRIEDEWALD Michael, PUNIE YVES, VILDJIOUNAITE Elena, AHONEN P., ALAHUHTA P., DASKALA B., DE HERT PAUL, DELAITRE Sabine, LINDNER A., MAGHIROS Ioannis, MOSCIBRODA Anna Agata, SCHREURS Wim, VERLINDEN Michiel, The International Library of Ethics, Law and Technology , 2008, Vol. 1,, published by Springer.

protection in relation to a decision, the Regulation establishes protection in the face of a measure. While the word 'decision' supposes that a judgment takes place (approving credit or fixing the price of health assurance for instance), the word 'measure' stands for any action toward a goal (e.g. using data correlation for marketing purposes). In this sense, the word 'measure' involves a larger set of actions, including the taking of decisions. Similarly, the Regulation links the protection not only to the evaluation of personal aspects, but also to the prediction of behavior. Having broadened the actions that are subject to its scope, the Regulation seeks to guarantee more protection to citizens than the Directive 95/46.

The third point concerns the list of exceptions. Article 20 of the Regulation uses a similar composition of Article 15 of Directive 95/46; i.e., as a rule, it forbids measures based on automated processing. But while the Directive previews two exceptions to this general prohibition – contract and specific law – the Regulation adds a third one: data subject's consent. Direct consequences relate to the conditions of consent. Considering that consent to profiling is different from consenting to data processing, data processors must ensure that distinguishable conditions exist for the data subject to consent to profiling, according to the Article 7,2 of the Regulation. Moreover, there is a clear correlation between profiling, consent and data subject's right of access. As stated by the Regulation:

> *"every data subject should therefore have the right to know and obtain communication in particular for what purposes the data are processed, for what period, which recipients receive the data, what is the logic of the data that are undergoing the processing and what might be, at least when based on profiling, the consequences of such processing"*.

How this correlation will be achieved is a question to be answered. It is true that the Regulation recognizes that the right of access will, for example, sometimes be confronted with trade secrets and copyright issues. It affirms that this confrontation must not imply a general denial of information about the logic or the correlations which are used for building-up the profile applied to the data subjects (number 51). But the Regulation does not go any further. Having opened the door to consent to legitimate profiling, the Regulation does not establish counterparts in favor of citizens: how to assure transparency with regard to profiling? What parameters to guide access to the information related to the logic of profiling? When data controllers will be authorized to deny access? The mere protection against a general denial of information is not only inconsistent with the transparency principle but is also imbalanced and far from satisfactory in protecting citizens.

9. Responsibility and liability

The effectiveness of legislation grounds itself on the obligations to respond to acts – responsibility – and to repair damage – liability.

Not explicitly mentioned by Directive 95/46, responsibility is plentifully established in the Regulation. With regard to the controllers, responsibility traduces itself into the adoption of policies and the implementation of measures to perform data processing in compliance with the Regulation (Article 22). These measures include implementing data security requirements and, for instance, performing data protection impact assessment. The Regulation also fixes the responsibility of joint controllers (Article 24), representatives of controllers not established in the Union (Article 25) and processors (Article 26).

Differently, liability is already considered by Directive 95/46, which establishes a liability regime based on compensating harm and presumption of fault. According to Article 23:

> "*any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered*". Moreover, "*the controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage*".

The Regulation introduces two substantial changes to this liability regime. First, it includes processors as liable for damages: being those who act upon data on behalf of controllers. Processors are highly engaged in data processing and for this their inclusion in the roll of liability is reasonable. Second, the Regulation establishes that "*where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage*". In effect, dilution of liability is a problem faced in data processing. Violations of personal data take place within scenarios of multiple actors in which it is difficult to identify the one at fault (technology creators, service providers, etc.) and the plurality of causes (data breaches, deficient design, etc.) adds an extra obstacle to determine liability. Establishing joint liability to controllers and processors removes from the shoulders of data subjects the burden to prove whose fault it is.

One last point, the Regulation imposes upon the actors mentioned in the previous paragraphs the duty to cooperate with the supervisory authority (art. 29) and notably to maintain documentation (art. 28) containing the different items of the 'notification' that are mandatory under the Directive, but only those necessary so as to alleviate the data controllers' administrative charges.

10. The regulation of technologies

Beyond the traditional mechanisms of responsibility and liability, the new framework opens the way in European law to the regulation of technologies, of which data protection by design, data protection by default and data protection impact assessment are three remarkable principles.

As regards the two first principles, the first one: 'Data protection by design'[8] is defined in the following terms:

[8] As asserted by Anne Cavoukian, DPA Commissioner from Ontario (Canada) in its introductory remarks to the Privacy Guidelines for RFID Information Systems available on the web site: http://www.ipc.on.ca: "*Privacy and Security must be built in from the Outset – at the design Stage*".

> *Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject* (Article 23.1).

Data Protection by design is the expression clearly inspired by the concept of Privacy by design (PbD), which "refers to the philosophy and approach of embedding privacy into the design specifications of various technologies". PbD applies "into the design, operation and management of information processing technologies and systems". An early reference to PbD is made in the Commission Recommendation of 12.5.2009, which establishes that privacy and security concerns must be built in radio-frequency identification (RFID) applications before their widespread use. Is the change from PbD to Data Protection by Design a specialization of meaning or will the expressions be considered as synonyms? Does Data Protection by Design imply embedding in technologies other values than privacy and security? How will the cost of implementation interfere with the responsibility of the controller? Given that the design of technology is essential in this approach why is there no reference to designers?

The second principle is also defined by the Regulation and claimed over a long period by privacy advocates. 'Data Protection by default' is defined by the Regulation in these terms (Article 23.2):

> *"The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals*".

Data protection by default is evidently related to the data minimization principle, according to which (a) processing non-personal data have preference over processing personal data and (b) if personal data processing is necessary, it must be limited to the minimum (Article 5,c). In this context, Data Protection by Default is a powerful instrument at the service not only of data minimization specifically but also of privacy in general, as it tends to give back to data subjects control over the disclosure of their personal data. In practice, for instance, it implies that in social networks, individual profiles should be kept private from others by default.[9] The data protection by default spectrum is large and may also affect contract practices. For instance, it can prevent service providers from unilaterally modifying their privacy policy to process more personal data.

In addition, the obligation to conduct Data Protection Impact Assessment[10] as a third principle, is established by Article 33,1:

> *Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

Data Protection Impact Assessment is thus defined as the evaluation "*of the impact of the envisaged processing operations on the protection of personal data where those processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*" (Article 33). Having taken into account the data subjects' views, as noticed by the Article 33.4, Industry and Governments have to evaluate risks not only as specified at the Article 33 on data protection but more broadly on the different liberties as mentioned at the Article 33.3 and on the human dignity of the data subjects in order to justify their decisions. Transparency of this previous risk assessment works as an important instrument to promote democratic debate through risk assessment since it promotes openness with regard to the decision-making processes.

Risk assessment is a procedure by which one distinguishes non-plausible from plausible risks and assesses the likelihood that these will occur. Privacy Impact Assessment (PIA) – which is at the heart of Data Protection Impact Assessment – is a sort of risk assessment since it aims to evaluate the potential consequences of an activity on privacy and data protection. Beyond the verification of legal compliance, PIAs "*have to consider privacy risks in a wider framework that takes into account the broader set of community values and expectations about privacy*"[11]. Consequently, PIAs are related to a form of political legitimacy of decisions concerning privacy and data protection. What balance will Data Protection Impact Assessment achieve with regard to "rights and freedoms of data subjects"? Is Data Protection Impact Assessment a parameter of a general duty of care? If yes, how will this determine responsibility and liability of actions according to this parameter?

11. Independent supervisory authority

The Regulation aims to enhance both the powers of the supervisory authorities and the consistency of their actions. According to the recent ECJ decision about the condition of the independency of the Data Protection Authorities, different detailed provisions (Articles 47 and ff.) are fixing rules guaranteeing this independency. As regards the powers, the Regulation, in its articles 52 and ff., creates uniform arrangements by upgrading them in certain countries: all the supervisory authorities will enjoy the competence to monitor, investigate and take decisions (including a ban on processing activities) on their own initiative or on a basis of a complaint coming from data subjects acting individually or collectively (see infra). If the Regulation suppresses the obligation of notification, which was considered an administrative burden,

[9] 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.", p. 23.

[10] On "Privacy Impact Assessment", see R. CLARKE, "Privacy impact assessment: Its origins and development", *CL&SR*, 2009, pp. 123 and ff. This article provides in two appendices a list of exemplars of PIA documents and references to guidelines describing different PIA methodologies.

[11] Warren et al. (2008, p. 235).

its counterpart imposes on data controllers of a certain size (more than 250 employees) a duty to designate a Data Protection Officer (D.P.O.), whose tasks and status are defined very carefully (Article 35 and ff.) under the present German model of the '*Datenschutzbeauftragter*'. The D.P.O will collaborate with the supervisory authority and in our opinion will guarantee a better internal understanding and effective application of the Data Protection principles within the data controller's organization.

The consistency of the actions of the supervisory authorities firstly is ensured by a rule of territorial competence in the case of a data controller having subsidiaries in different European countries. The competence in these cases is exercised by the Authority where the main establishment of the data controller is located. Its decision, according to the obligation to notify the draft measure to the other supervisory authorities concerned (see the procedure just below), is enforceable in all Member States (M.S.) concerned. Furthermore, the Regulation (Article 55) obliges each M.S. supervisory authority to cooperate with one other. One last point: the consistency is achieved by a strong competence granted (Article 58) to the European Data Protection Board which is the successor of the less powerful Article 29 Working Group (W.G.) of the Directive 95/46. The draft measure must be communicated to the Board but also to the Commission. The famous Article 29 WG is thus replaced by an "European Data Protection Board" (EDPB), with the same composition but entitled to be alerted each time an envisaged national DPA measure will affect the Trans-Border Data Flows (TBDF) or data subjects located in another or several other countries.

So the Board might intervene each time a national supervisory authority intends to take a decision which might affect data subjects or data controllers located in another country. The opinion delivered by the EDPB might be followed by an opinion of the EU Commission in order to ensure correct and consistent application of the Regulation or/and by a decision of the Commission to suspend the draft measure. We underline the strange role played by the Commission according to Articles 59, 60 and 61, which enact that in a last resort the Commission may adopt an opinion to ensure '*correct and consistent application of this Regulation*'. Such opinion must be taken into '*utmost account*' by the supervisory authority otherwise it may see its measure suspended.

12. Collective protection of personal data

Privacy and data protection laws frequently undergo violation with many legal wrongdoings, typically mass exposure torts.[12] Bringing a case before an authority is costly, which is a circumstance that inhibits people from defending their rights. One procedural mechanism to improve the enforcement of legislation and the protection of rights of victims is "collective redress", which allows people to claim in a single collective redress procedure or through a representative entity or body acting in the public interest.

In the Regulation, the framework of collective redress is twofold: administrative and judicial. It permits data protection NGOs to lodge complaints with a supervisory authority (Article 73,2) and to claim judicial remedies (i.e., class actions) against the supervisory authority, controllers and processors (Articles 74, 75 and 76,1). NGOs are allowed to do this on its behalf or on the behalf of one or more data subjects. Having introduced collective redress into the general data protection framework, the Regulation takes a significant step to enhance the protection of citizens' rights. Further developments are needed, notably civil procedure rules to shape the operation of collective redress. For instance, in converting individual proceedings into collective action what will be possible? What consequences arise in opting for an individual procedure or a class action? The responses to these and other questions will depend not only on the legislative progress coming from Member States but also on the outcomes of the European Commission's initiative on a common framework for collective redress.[13]

13. Transfer of personal data to third countries or international organizations: many open doors?

The regime of international transfer of personal data will be significantly altered by the Regulation. Here we emphasize the general principles, effectiveness of data protection and new modalities of transfer.

The Regulation allows transfers to third countries, as the Directive 95/46 does, but also to international organizations. Under Directive 95/46, transfers request that the third country assures an adequate level of protection of personal data. In contrast, the Regulation demands that its protection framework must not be undermined with the transfer. Controllers and processors involved in the transfers must comply both with the rules related to the transfer as well as with the other provisions of the Regulation (Article 40).

The Regulation brings important novelties to improve effectiveness of data protection in the context of transfers with an adequacy decision. While assessing the data protection adequacy level afforded by a third country, the Commission must take into account not only the outline of the rule of law – as within the Directive – but also new important elements concerning the existence of effective and enforceable rights to protect data subjects, the effective functioning of an independent supervisory authority and the international commitments the third country or international organization in question has entered into (Article 41, 2, a, b and c). Going beyond the formality of a rule of law assessment, this approach clearly emphasizes practical concerns about data protection. For this reason, it tends to give stronger responses to privacy concerns.

[12] For instance, the American Online (AOL) 2006 data leakage incident released data that included 20 million web queries from 650,000 AOL users. Likewise, when Facebook decided to change its terms of service to claim ownership over any user content on their site, it had 175 million active users (today it has more than 845 million). Sources: http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data, April 6th 2011, http://edition.cnn.com/2009/TECH/02/17/facebook.terms.service/index.html, April 6th 2011 and http://newsroom.fb.com/content/default.aspx?NewsAreaId=22, April 6th 2012.

[13] See the works of the European Commission on a common framework for collective redress, http://ec.europa.eu/consumers/redress_cons/collective_redress_en.htm, 7 March, 2012.

Under Directive 95/46, the adequacy decision from the Commission is the modality par excellence to transfer data. Alternatives to transfer data are presented in a derogation regime (Article 26), of which transfer by adequate safeguards are an example. These safeguards may result particularly from contractual clauses. Coupled with derogations to the regime, the Regulation creates new modalities of transfer, which are presented as a second best with regards to the adequacy decision. This means that the adequacy decision is still the primary method of undertaking international data transfers. With regard to secondary options, the "adequate safeguards" of the Directive become an enriched framework in which data transfers can be accomplished through binding corporate rules, standard data protection clauses adopted by the Commission or the supervisory authority, and contractual clauses between the controller or processor and the recipient of the data authorized by a supervisory authority (Article 42, 2). New modalities are a synonym for more flexibility to the data transfer regime, which favors free movement data. How this flexibility will affect data protection is a question to be answered once the law is put into practice.

Despite of this uncertainty, and particularly concerning the derogations regime, two points deserve special attention. The first concerns the extent of the derogation regime itself. While in the Directive the derogations are limited to "*particular cases*" (Article 26), such restriction does not exist under the Regulation (Article 44). The second relates to the transfer authorized by consent. The Regulation states that a transfer can be done "*if the data subject has consented to the proposed transfer,* ***after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards***". Here, it is worth noting that the set of options available to controllers and processors is quite enlarged. Even without an adequacy decision or any of the four alternative modalities, controllers and processors will be still be able to legitimate and sign off data transfers; it is enough to obtain the consent of the data subject, on whom the burden of risk will be placed. Doing this, the Regulation opens the possibility to ground the legitimacy of a data transfer exclusively on consent, even without safeguards. The text is contradictory to Article 7,4, which states that consent "*shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller*". It is also contradictory to the very essence of the Regulation since transferring data without safeguards is a synonym for transferring with no data protection.

14. Conclusion

This paper glimpses into the new data protection regime brought about by the proposed Regulation of 2012. After all said and done the search for a more flexible and effective legislation demands double attention. Looking back, we should not disregard the fact that data protection is more than a set of data processing rights; it is an outcome of a process of protecting individual freedoms in our Information Societies. Looking forward, putting the Regulation into practice, demands using new important tools such as the transparency principle, the joint liability rule and data protection impact assessments. We must do all of that without disregarding the point that the paramount function of the data processing framework is to protect citizens.

The question therefore is whether the drafted Regulation offers an adequate answer to the concerns we have as regards the survival of our liberties in the Information Society? Multiple positive points can be identified in the draft Regulation. We do appreciate the new rights granted to the data subjects and the possibility of collective action. We can also emphasize the enlargement of the duties and the increasing liability of the data controllers. In principle, the techno-legal approach (data protection by default, data protection by design) and the duty to initiate a data protection impact assessment are appropriate tools for ensuring the effectiveness of the proposed protection. But at the same time it introduces reliance upon technical expertise to solve societal debates if there is no real debate as regards these technical choices. The increasing roles and competences of the data protection authorities might be considered as positive but at the same time, as denunciated by Flaherty in the eighties, it creates a risk that our data protection authorities will be more afraid to take privacy friendly positions and more desirous to play an administrative role. The Commission has been definitively empowered with new roles and as developed will be the major player in the implementation of many of the provisions in contrast to Member States.

The need for a consistent and uniform approach is the main legitimate justification both for ensuring the correct functioning of the internal market but also for defending the European position vis-à-vis the rest of the world. At the same time we fear that harmonization will hinder fruitful competition between the Members States' approaches and solutions which would otherwise benefit our liberties. Finally, as already asserted, we deplore the fact that the reference to the right to Privacy has been deeply cut off and that data protection is now considered as a constitutional principle *per se*. It must be feared that the link with the quite innovative jurisprudential developments of the Strasbourg Court and the preeminence of the libertarian approach will be favored and that the implementation of the Regulation will lead to no more than a simplistic balance between different contradictory interests.

Luiz Costa (*luiz.costa@fundp.ac.be*) *Researcher at the CRIDS (University of Namur), Federal Prosecutor at São Paulo.*

Yves Poullet (*yves.poullet@fundp.ac.be*), *Rector of the University of Namur, founder of the CRIDS.*