COMPUTER LAW & SECURITY REVIEW 34 (2018) 773–778

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Is the general data protection regulation the solution?

Yves Poullet[a,b,*]

[a] Namur Digital Institute, University of Namur, Belgium
[b] Universite Catholique de Lille, France

ARTICLE INFO

Article history:

Keywords:
GDPR
e-Privacy Directive
Co-regulation
Data protection or privacy
Democracy, liberties, social justice and dignity as key concepts of privacy
Consent
Profiling
Right to be forgotten
Concept of personal data-alliances with other legal branches

ABSTRACT

Never has a text been received with so many requests for amendments; never has the debate around it been so huge. Some see it as a simple duplicate of the Directive 95/46; others present the GDPR, as a monster. In the context of this birthday, it cannot be a question of analyzing this text or of launching new ideas, but simply of raising two questions. I state the first as follows: "*In the end, what are the major features that cross and justify this regulation?* In addition, the second: "*Is the regulation adequate for today's digital challenges to our societies and freedoms?* The answers given in the following lines express the opinion of their author. It is just an invitation for a dialogue to go forth in this journal where so many excellent reflections have been published on Digital Law, thanks to our common friend: Steve.

1. Main lines of the regulation

Four main trends appear to me to clarify the provisions of this regulation. The first is the aim to define once and throughout the world, a totally or quasi-totally unified and coherent European model of data protection, particularly in contrast to the American model. The European model, which is its second virtue, intends to take into account the unprecedented technological developments that have occurred since 1995: that is to say the year of the adoption of the directive, and their impact on the data protection. To this "technological revolution", are added, the third line of force, namely the requirements of our European legal system which, since 1995, did not hesitate to create a quasi-constitutional right to data protection and which the judges did not cease interpreting in a bold way. Lastly, comes the fourth point arising from the European text, viz the major concern of the authors of the text to reinforce the effectiveness of the legal rules as expressed by the GDPR. Let us develop briefly each of these four points.

* Namur Digital Institute (UNamur), Université de Namur, Rue de Bruxelles 61, 5000 Namur, Belgique.
E-mail address: yves.poullet@unamur.be

https://doi.org/10.1016/j.clsr.2018.05.021
0267-3649/

1.1. *Towards a unified and coherently applied model of data Protection: a regulation and no more a directive*

The choice of a regulation as a fixed legal instrument, leaving little if no margins of manoeuvre,[1] and not of a directive is explained[2] by the will of the EU authorities to fight against the fragmented implementation of the Directive 95/46 by the national provisions and their divergent interpretations. Furthermore, the point is underlined that the GDPR intends to be much more precise than the Directive: 99 articles instead of the 34 articles of the Directive and that without taking into account the numerous Guidelines.[3] These Guidelines, already partly enacted by the Article 29 Working Group are designed to interpret any flawed concepts or add clarity to certain provisions, which will have to be followed by the recipients.[4] Beyond that first element, it is clear that the Regulation affords to the future "*European Data Protection Board*" (Article 68 and ff.), powers without comparison to those of the previous Article 29 Working Group and considers this Board as a unique body in charge of the GDPR interpretation. In the same perspective, Article 92 confers to the E.U. Commission the power to take delegate Acts, which will still contribute to the European standardization of data protection.

To ensure a coherent GDPR application, the text provides not only the criterion to determine in the role of the supervisory authority in relation to transborder data flows, but also the way by which the divergences of interpretation between Data Protection Authorities (DPA) have to be solved. That designation will contribute to the effectiveness of the intervention and the procedure to solve possible divergent solutions and help to maintain the consistency of the GDPR implementation.

The European Union intends to affirm this model throughout the global world, for the GDPR extends the territorial scope of its application beyond the European borders. It does so by moving away from the flawed approach provided by the Directive to a more adequate one: viz. a focus on individuals within the EU. This criterion applies the GDPR to companies or other data processors every time they target European Union residents, by offering goods or services or follow-up to their actions (Article 3.2). Furthermore, in the case of transborder Data Flows, the GDPR strengthens the criteria for considering third countries' own rules as adequate by claiming in particular the existence of international engagements and the existence of an independent DPA, whether public or not. One also notes the European insistence that if alternative solutions have to be found to allow a transborder Data Flow, that solution must ensure "*appropriate safeguards*" for European data subjects, such as "*enforceable data subject rights and effective legal remedies*" (Article 46).

1.2. *The adaptation to the requirements of the evolution of the digital world*

To the hardly nascent Internet of the year 1995, one compares the existence now of a global and ubiquitous web combining both the infinitely large capacities of our computers (Big Data), our networks and the infinitely small 'chips' lodged in our pockets, in our glasses, in objects or even in our body and brains. The applications are multiplied, thanks to the Internet of Things, cloud computing, genetic manipulation and the contributions of nanotechnology, biotechnology, information technology and cognitive sciences (NBICs). The development of artificial intelligence more and more animates our robots and already opens up the prospect of 'trans-humanism' envisaging the fusion of the brain and the computer. The GDPR intends to take into account this new digital world and these 'revolutionary' applications. Online identifiers, such as location data, are cited among personal data, biometric and genetic data and are listed from now on as sensitive data. Provisions on profiling, born of artificial intelligence, are enacted and the Recitals mention in different places the application of provisions to particular technologies. It is obvious that the advent of these technologies significantly modify (Recital 6) the methods of the collection, processing, storage and exploitation of personal data. Whether the regulation does that sufficiently and properly, is another question? We will come back (infra, 2.2) to that question.

At the same time, technological progress might also benefit from the better implementation and effectiveness of Data Protection as technology can contribute to the cause of data protection. In this respect, I pinpoint two principles: the first is the reciprocity of the advantages. It means that to the extent that data controllers can take advantage of technological applications, to facilitate data processing for their own purposes, then to the same extent should data subjects be enabled to take advantage of the technologies too in order to exercise their rights. These include notably the withdrawal of consent and other rights to their information and access. A second principle can be deduced from the provisions about 'privacy by design' or 'privacy by default'. Embedding data protection at the heart of the technology to ensure the respect of the legal provisions, is definitively a challenge that the GDPR aims to take up.

1.3. *The adaptation to the evolution of the legal context*

In 1995, the authors of the Directive based their intervention on the need for creating an interior market for the free move-

[1] However certain margins of manœuvre still exist for example, with regard to the regime of the sensitive data (Article 9), as regards the press (Article 85), the access to the official documents(Article 86), as regards business relations(Article 88) This possibility of divergent applications especially exists with regard to the public authorities processing. Each member-state will be still able to model, in an original way, the public sectors processing admittedly in the limits of the general principles enunciated at Article 5. At my opinion. the uniformity gained by GDPR is likely to be more present for the private processings than for those public ones.

[2] Recital, no 9.

[3] See the 10 Guidelines already issued (from April 2017 to February 2010) by the Article 29 Working Group settled up by the Directive 95/46 and joining a representative from each national Data Protection Authority published on the art. 29 website available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[4] Topics or questions like Consent, Data Protection Officer, Privacy Impact Assessment, Data Security Breaches are so 'regulated' by these Guidelines. It is quite clear that these Guidelines, even they are necessary due to the lack of clarity of certain GDPR provisions create difficulties of legibility of the applicable norms.