Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Is the general data protection regulation the solution?

Poullet, Yves

Published in:
Computer Law and Security Report

DOI:
10.1016/j.clsr.2018.05.021

Publication date:
2018

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

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2018, 'Is the general data protection regulation the solution?', *Computer Law and Security Report*, vol. 34, no. 4, pp. 773-778. https://doi.org/10.1016/j.clsr.2018.05.021

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 08. Jan. 2025

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.

© 2018 Yves Poullet. Published by Elsevier Ltd. All rights reserved.

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/© 2018 Yves Poullet. Published by Elsevier Ltd. All rights reserved.

tions, making them responsible in front of the judges in the event of exaggerated zeal.

2. The RGPD, an adequate regulation?

This second part of the discussion intends to be more critical. Criticisms will be made in two forms. The first collects a certain number of remarks that I qualify as 'pointillist' ones.[8] Therefore, the question of consent, its nature and its impact deserves some reflection. I will discuss the definition of personal data and address some reflections about the not very clear regulation of profiling activities. Then, I will underline, based on some provisions of the GDPR, the invitation to enlarge the Data Protection debates to new alliances with other branches of the Law, especially consumer, environmental and competition Law. Lastly, I reflect upon the reasons why some advances of the e-Privacy Directive have not been taken up within the GDPR provisions.

The second form of criticism is more fundamental: it relates to the drafting of GDPR Article 1.2. Ultimately, the question is whether the concept of Data Protection is taking adequately into consideration the real challenges of our digital world.

2.1. *About some 'pointillist' remarks*

With reason, the GDPR authors – and since the Article 29 Working Group comments – have reinforced the conditions of the giving of consent, one of the legitimate bases of lawful processing. Questions are still pending however: is it necessary, for example, to maintain consent as a necessary and sufficient basis for defining the legality of certain processing? The first data protection legislation or treaty (see, in particular, Convention no 108 of the Council of Europe) did not introduce it. However, Article 8 of the Charter expressly lays down additional safeguards for legitimate consent even if these are rarely met. In the Internet context, which aspect of consent can be said to be free, specific, informed and unambiguous? One must conclude that the consent given individually by data subjects remains a false premise when up against the social need represented by the need for access to the Internet and to certain services (social networks, search engines, etc.). In that context, on one hand, I suggest that it would be useful to introduce the idea of collective negotiations between data subjects (or their representatives) and the data controllers. On the other, as regards certain services of great necessity, such as access to social networks or to search engines, we plead for an a priori regulation of the processing generated by their use. Staying with the issue of consent, it would be also be useful to answer another question: *"Does the consent make possible a processing beyond the basic principle of what is proportionate?"*

My second point deals with the concept of personal data in personal matters. There are two reasons for this focus. The first comes back to an argument that I have been developing since 1979, outlining certain legislation that has extended Data Protection to legal persons. I submit that it is necessary now to return to this issue. The e-Privacy Directive is doing so but more generally speaking, should we not now be considering the greater asymmetry that exists between the informational power of large companies, or companies using Big Data, in order to profile other companies, including small and medium enterprises (SME). Surely, these practices justify the need for protection of the legal entities concerned. This protection is founded both upon the right of SME's to participate in such profiling, but also upon the need to protect their employees. By enlarging the protection to SME, it would be possible for them to enjoy certain prerogatives of the data subjects: right of access, right to be forgotten, right to erasure, etc.

Another aspect relates to the dangers of restricting the protection only to personal data thereby excluding anonymous data, the use of which is increasingly frequent particularly in the Big Data applications. Not only it is far from being obvious that anonymity can resist the massive and cross analysis of quantities of data but, moreover, when combined with 'personal' data, they acquire, by their use, the quality of personal data. Furthermore, they can induce, in operations of profiling, not only individual but also collective discrimination.[9] Article 4 (1) defines personal data by their content, per se. In my opinion, 'personal data' has also to be defined by their use. In other words it is the processing and their possible impact on a data subject individualized (not necessarily identified), which reveals whether data is personal or not.[10]

Profiling is evoked in at least in three articles: 13, 15 and 22 but its regulation does not seem to be satisfactory to protect effectively the data subject. The essential question for the latter, upon discovering that they been submitted to profiling, goes beyond a simple request either not to be profiled in the future or to reject the decision taken under the 'sole' basis of his or her profile. What the data subject wants is to understand the criteria taken into account for the profile. In other words, he or she wants to enjoy transparency of the algorithm, which leads to this result and the data retained, taking into consideration the factors that have been taken into account. However, as shown above, anonymous data are not taken into consideration as overall; the GDPR mentions the right of access (Article 15) in terms that only *"useful information concerning subjacent logic"* has to be provided. It is somewhat short of what is needed, especially when it is known that the person in charge of processing can still call upon rights to the secrecy or the intellectual property to reduce the useful information.

[8] Pointillism is a technique of painting in which small, distinct dots of colour are applied in patterns to form an image. See https://www.widewalls.ch/pointillism-dotted-art/.

[9] This point is important. In case of profiling activities or automated decisions, the data controller has to reveal only the categories of personal data he is processing ... and not the anonymous data. But the weight of these anonymous data might play a crucial role for defining the profile and understand the logic of the processing.

[10] It is noteworthy to underline that the GDPR (Article 9) has modified in that sense the definition of sensitive data: As clearly showed by the French GDPR version (*'traitement de données qui révèle'*) it is the processing of data which reveals the sensitivity of the data and no more the content of the data in itself. So a video showing handicapped people is not a medical data if the processing of these images is not aimed to notice the handicap but for instance only to control the people entering into a building.

Two provisions introduced by the Regulation invite the supporters of data protection to seek alliances with other actors involved in other branches of the right. One is already evoked; viz., the introduction of a kind of Class Action, suitable for consumers' rights and taken again by the GDPR, creating an alliance with promoters of consumer protection. Another is the provision dealing with the portability of data (Article 20), which is clearly also a rule coming from competition Law, stimulating a more healthy competition environment. The objective of this provision is as much about the protection of the data subject as the stimulation of healthy competition. The point is simply to underline the interests with which the cause of data protection could seek synergies to protect data subjects against dominant position abuses, or undue concentrations.

The e-Privacy Directive incorporates, after the first Data Protection rules and Directive 95/47, a third generation of data protection legislation.[11] I wonder why the GDPR has not chosen to adopt certain e-Privacy principles. I mention two examples. The first relates to the prohibition, other than by consent of the user, to store information or to reach the information stored on the user's equipment. This principle establishes a kind of data subject right to the protection of his or her 'virtual house', which is quite important at a moment given the ubiquitous nature of information and communications technology (ICT). The second example is Article 14 of the e-Privacy Directive, which grants to the EU Commission the competence to establish technical standards designed to guarantee the conformity of the equipment to the Directive's requirements. This provision applies potentially to all infrastructures, terminal equipment and software and would have been useful within the GDPR. Indeed, it is a pity that the GDPR considers only the relation between data controllers and data subjects and neglects the role of the technical interface between these two actors. Therefore, technical norms presently permit the existence of invisible hyperlinks, which authorize the redirection of a visit by an Internet user to another site, other than the one visited, and for this first site to send its own cookies. Deficiencies of transponder security will permit third parties to have access to the data stored in a Radio-frequency identification (RFID) device. In other words, it is a matter of regret that the Regulation does not foresee, apart from the data controller's responsibility, a direct liability upon producers of the infrastructures, terminals and services like the software, despite requests to impose this by the Article 29 Working Group. Furthermore, the GDPR does not envisage a system of technical norms, certification or labels in order to ensure the conformity of the terminal equipment and software application with the legal requirements: an unhappy gap that one!

2.2. Is *data protection the right way for protecting 'netizens' in our digital societies?*

Article 1.2 fixes, in a laconic way, the objective of the Regulation: "*This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data*". Admittedly, through the GDPR provisions, limits put on the use of personal data are fixed and data subjects interests and liberties prevail over those of the data controllers, but questions remain: *"How to make that balance?* in addition "*...according to which criteria: individual or societal? "In the second case, which ones?"* Let us take an example drawn from a recent experiment: an insurance company proposes a significant reduction to my car insurance premiums if I agree to accept the installation of an 'informer' in my car, which can attest to my adherence to the Highway Code and road traffic legislation. It is probable that I will not identify any objection to such a proposal and that I will readily agree to the insurance premium reduction. However, this method of calculating insurance premium rates, derogates from the traditional design defended by the insurance sector, namely the mutualisation of assured risks. In short, the weighing of interests and liberties can and must, in certain cases take place, not at the individual level, but by taking into consideration societal issues and values too.

This assertion remains strong when one considers data processing related to the genetic manipulation of data, where it is a question of human identity and discrimination of access to this kind of activity or due to profiling based on such genetic data. Likewise, the recent European Data Protection Supervisor (EDPS) opinion on online manipulation[12] demonstrates clearly that other questions concerning protection of individuals are also at stake, particularly our democracy's requirements. In other words, the data protection debates demonstrate ever more strongly the ethical questions of social justice, democracy, dignity and, non-discrimination.

In this context, one must oppose the poverty of the expression retained by the European Regulation, in the text of Article 1.1 of the 1978 French Act "Data-processing and Freedoms": *"Data processing must be with the service of each citizen. Its development must take place within the framework of the international cooperation. It should carry reached neither to the human identity, neither with the human rights, neither with the private life, nor with individual freedoms or public"*.

Should our Data Protection Authorities be entitled to instruct and to decide these debates and play a role close to Offices of Technology Assessment and, if necessary, according to the precautionary principle, to alert people in case of risky technological developments? Society needs to address problems like the progressive obliteration of political deliberation by an "algorithmic governmentality"; the standardisation of the behaviours by an insidious technological normativity; the increasingly exclusive taking into account of the data compared to the account and the meeting of the people; and the ethical questions of the increased use of bioengineering applications. Lastly, one wonders how our Authorities can embrace these fundamental societal issues, raising the fundamental question: how can technological development promote dignity and the blooming of the personality in a democratic soci-

[11] On this point, see our developments in 'About e-Privacy Directive. Towards a third Generation of Data Protection Legislation», in *Data Protection in a Profiled World*, Gutwirth et alii (eds), Springer, 2010, p 3 à 30.

[12] Opinion 3/2018 (March 13, 2018) available at the EDPS website: https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf. This opinion is particularly welcome just at the moment of the Cambridge Analytics/Facebook scandal where against two dollars, Facebook customers have accepted to give access to their Facebook data.

ety, elements of which are, according to the Strasbourg Court of Justice case law, at the core of the Privacy concept?

That our Data Protection Authorities should participate in these debates is certainly important, but they must not in effect confiscate the debate through Committees of Ethics and Sciences, of bioethics, of Technology Assessment. Instead, they must carry these issues into an open, public and democratic debate. The importance of the debate exceeds by far the somewhat restricted debate about weighing the individual as against companies or the general public interests, to which the GDPR exclusively focuses, if at least one follows the poor wording of Article 2.1. In our opinion, Data Protection or rather Privacy can never be anything other than a tool at the service of freedoms, social justice and non-discrimination. Let us take again into consideration the matter of French law. It clearly affirms the duty to place technology at the service of humanity i.e. his or her identity, dignity and freedoms.

Precisely at this point, I would like to come back to the Privacy concept. In my opinion, it was not a good idea for the European Union to separate Privacy and Data Protection, even if the term Privacy induces a restrictive and negative approach: the "right to be let alone". The Privacy concept is a broader concept. German constitutional case law bases Privacy separately from that of Data Protection legislation in two constitutional principles: Human dignity and the blooming of our personalities in an evaluative societal context. To be short, let us recall that the Strasbourg Court of Justice notably in the Pretty case[13] said this:

"As the Court already had the occasion to observe it, the concept of "Privacy" is a broad concept, likely of an exhaustive definition. It covers the physical integrity of the person (...). It can sometimes include aspects of the physical and social identity of an individual (...). Elements such, for example, as the sexual identification, the name, the sexual orientation and the sex life concern the personal sphere protected by Article 8 (...). This provision also protects the personal right to development and the right to establish and maintain the relationship with other human beings and the external world (...). Although it was established in no former business that Article 8 of Convention comprises a right to self-determination as such, the Court considers that the concept of personal autonomy reflects an important principle, which underlies the interpretation of the warranties of Article 8".

So Privacy must be understood, not as a purely individual claim, which excludes others, but quite the opposite, as that of a person responsible for his or her own development. This development requires the existence of two different rights, which appear at first glance to be contradictory to one another but in reality are complementary. The first one is the right to "seclusion"[14] which means the choice of the individual to decide when to retire from the world at large. The second one is that of entitlement to membership of the society and the opportunity to enter into multiple interrelationships with other members of it, by the right of "inclusion". It means to be able to take part to our democratic society fully and without undue constraints or manipulation. Data Protection is nothing more than a tool to ensure Privacy and is a pre-condition of all our freedoms and our dignity. If we place Data Protection on a pedestal, and separate it out from the concept of Privacy, this will reduce the question embedded in our digital universe to one based purely on a debate about legal techniques and terminology without any soul or sense of direction.

Author Information

Emeritus professor at University of Namur, Associate Professor at the UCLille, Co-chairman of the Namur Digital Institute (UNamur). Université de Namur

[13] *Pretty vs. UK*, Case n° 2346/02, April 25th, 2002.

[14] This possibility of withdrawing him or her self "between the four walls of his or her house"undoubtedly would need a new dedication at the time of the ubiquity of the Internet. On that point, one refers to the "right to be forgotten" enacted by the GDPR but we suggest also the "right to a (relative) anonymity" (with exception for requirements of public and thirds' security) and the "right to log out", to be disconnection from the digital infrastructure as it was enacted by the former ISDN Directive and finally the "right to our digital home", the right to have no intrusion from outside in our personal digital equipments, enacted by the e-Privacy Directive (Article 5).