Data protection or privacy ?

Poullet, Yves

Published in:
Deep diving into data protection

Publication date:
2021

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

Data protection or privacy?

Yves POULLET[1]

As a retired academic, I feel authorized to be a bit provocative in front of a 'Data Protection' (and no longer a 'Privacy') advocates' audience.

To be short, I will say: "In the future, what we definitively need is more privacy and perhaps less data Protection"?

1. Preliminary reflections about the two concepts – Privacy, as J. COHEN explains, constitutes a misleading **term** since at first glance and after a first reading of our ECHR' article 8, the concept of Privacy seems to refer to the right to be let alone by other people, including the negative right to forbid processing by others. But today, if I analyze the Strasbourg Court case law (notably, the *Pretty*, *Botta* & *Barbulescu* cases), Privacy has another dimension. It encompasses all the conditions public and private authorities have to guarantee in order to ensure the self-development of human beings in a still evolving societal context and at the service of our democratic societies. According to the Court, Privacy might be defined as the right to self-determination, or as I prefer to call it, the right to self-development. It gradually encompasses all the conditions which might reasonably be needed for an individual within a determined society to "build up his or her own identity". In other words, Privacy means both the right to be let alone and the right to act positively within the society, freely, by mastering our informational environment. The right of seclusion and the right of inclusion constitute two intertwined facets of the same fundamental rights. You could never imagine that a person might be able to self-develop if they had, at the same time, the possibility to free themselves from their environment and to circulate with a minimum of trust and control by him or herself within an information society.

Data Protection (D.P.) might be a misleading **concept** at a time where the challenges posed by the growing digitalization of our societies are of societal and ethical nature. Indeed, DP legislations are based on an individualistic approach (see, the preeminent role of consent as basis of a lawful processing) and are focusing on the personal data subject's

[1] University of Namur, Faculty of Law, CRIDS/NADI. The text has been presented at a conference organised by the VUB, in Oktober 2019.

relationship to his or her data[2] at the detriment of the public interest. I take only one example: your car insurer suggests that your premium be determined in accordance with your driving behavior, calculated by an A.I system nourished by the data recorded by different data sensors installed within your car. Your consent definitively meets your economic interest but at the same, it raises the question of the 'risk pooling' principle, which is fundamental in the insurance sector, thus causing harm to other people (candidates to the same insurance) and the public interest.

So, when you refer to the connection or complementarity between DP and Privacy, I prefer to talk about hierarchy. From my point of view, it is absolutely necessary to assert that our DP regulations, in particular the GDPR, are only derived regulations from Privacy requirements at a precise moment in the technological development. Fully taking into account the Privacy requirements facing the risks linked with our present and future technological developments, it would be important, in my opinion, to design new generations of privacy legislation or at least new avenues for interpreting data protection legal provisions. The GDPR, with all its well-known qualities, is certainly not the holy Bible, but only acts as a point of departure at a precise moment in the technological development.

2. The GDPR facing new technological developments: some concerns – Indeed, it is obvious that our GDPR has certain difficulties to meet the already existing challenges raised by new digital applications and shortcomings. I take different examples:

a) **Artificial intelligence or robots** are raising a lot of questions about GDPR applications. I list certain of them:

- Where is the proportionality principle since we know that AI profiling systems, especially deep learning systems are using a lot of data, without knowing their relevance?
- How to ensure the respect of GDPR provisions as regards the processing of data concerning third parties (for instance, the collection of data about the nurses or the visitors of patients by a robot helper care-giver)?
- The approach taken by personal data is clearly not sufficient at a time where big data are using both anonymous and non-anonymous data, and where the distinction between both categories is flawed.
- How to ensure transparency of the "logic when we are using 'deep learning AI systems', based on random correlations"?

[2] This relationship is even analyzed by certain authors as a kind of property.

– Sensitive data, as Cambridge Analytica revealed it, must not be considered *per se* but in consideration of the processing purposes.

But overall, as asserted recently by the CoE Guidelines on AI and DP (Jan. 2019), AI and robots challenges lead us to considerably extend the scope of our reflections, far beyond and above DP: "We should consider not only human rights and fundamental freedoms but also the functioning of democracies and social and ethical values."

b) **Digital Content services** – Recently, the discussion raised by the Directive on Digital Content services, which was just enacted, about the so-called 'gratuitous' Digital content services and the problem of their effective use of 'counter-performance' by consumers through the provision, to Data Controllers, of their data has clearly revealed the difficulty to apply the GDPR ever since:

– 'Consent' viewed as the privileged ground for legitimating data processing is, in most of the cases, an illusion and does not offer adequate protection to DS or consumers
– There is a need for a consumer's privacy approach based on a preliminary collective discussion between the provider of these services and consumers' associations.
– Certain services 'offered' by communication or information platforms might be regulated since they constitute 'universal services', needed to ensure a social life for every citizen.

c) **The blockchain applications** – As asserted by a number of DP specialists, it is far from easy to solve questions raised by blockchain applications in the context of the GDPR. How is it possible to ensure, within blockchain context, the right to delete or to correct my personal data? How is it possible to ensure the proportionality as regards the duration of the processing? Once again, we will have to consider innovative ways to find solutions, and more than likely beyond the GDPR.

d) **NBIC and Genetic data** – Last point but not the least one: the processing of genetic data in the context of NBIC applications raises certain questions as regards the application of the GDPR. The GDPR considers Genetic data as personal data but they are also shared data within a family or an ethnic population, and their processing definitively is of general interest for research and healthcare improvements in the health sector. Moreover, the GDPR proves unable to solve the numerous fundamental questions we face considering the possible manipulation of genetic data and the increased man promised by these developments. We may point out the problems of discrimination as regards the access to new health services linked with new technologies, the problem of the future of our mankind, or the limitations of our ability to determine the genetic baggage of our progeniture.

3. What do we need in the future? These examples show very clearly that we definitively have to go far beyond Data Protection provisions, if we want to correctly address the challenges we will face tomorrow as regards the future of our societies and liberties. I totally agree with EDPS Giovanni BUTARELLI when, at the inaugural session of the 40th International DP commissioners' conference, he considers and asserts that Ethical values must, from now on, constitute the main aim for our DPA reflections and actions. I mention the fundamental ethical values internationally recognized and raise certain questions apart from them.

a) **Dignity:**

- against datafication of our lives… we can never be reduced to our data (see UNESCO Convention on Bioethics);
- the right not to be subject to the 'truth' of our computers…
- the need to regulate 'nudges' or digital manipulations (idea of protection of a mental health privacy)
- the duty to inform about the robot's presence

b) **Autonomy**, not in the sense of a 'robinsonian' liberty but as a liberty taking into account the liberties of others:

- the right to transparent or at least explainable AI and Information systems more generally
- against the invisible normalization of our behaviors, the obligation to develop possible choices (interoperability, right to different ways to get a service)
- the right to be disconnected and to have our computer protected as a virtual home

c) **Social justice:**

- The duty to take into account the 'general interest' and the impact to other data subjects in our privacy Impact assessment
- The duty to fight discrimination: in my opinion, this question will become a major problem due to AI predictions and the possible discrimination, as well as the risks of bias implemented into our AI systems, through the cost of the access to the new services (particularly as regards health or educational services).

d) **'DO GOOD and DO NO HARM'**

- Beyond 'Privacy by design', 'Ethics by design' of our digital societies. But also, the need to designate IS producers and designers and not only Data controllers as 'accountable' for this design.

e) The need for a collective assessment by all stakeholders and the need to take a precautionary approach (Digital environment) when faced with disruptive innovations like blockchain, smart cars, AI, etc.

f) A 'sandbox' approach: due to the difficulty to measure the social impacts of new technologies and their often radical unpredictability, it means – in the context of experiments authorized by a legislation – setting up a system of evaluation and control including by DPA, in order to then take decisions on a more permanent basis.

SELF DEVELOPMENT AND DIGNITY must be the KEYWORDS in the future and this should apply beyond DATA PROTECTION.

4. The need for new alliances – As privacy advocates, in order to achieve our mission to ensure the 'capabilities' (A. SEN), in other words, the self-development of all citizens, we have to seek new allies. We are not alone in these debates: bioethics, consumer protection, environmental, civil liberties, technology assessment commissions and associations, should all join their forces in this reflection. It is only through our common and coordinated efforts that we will help people and the society in general to master the development of a better digital world.

Another point to which we must pay attention is the multiplication of conflicts between Human Rights caused by our digital world: between Intellectual Property and D.P.; between Freedom of expression and DP; between freedom of undertaking and D.P. On that point, I do regret that we are faced with a multiplication of human rights; D.P. has been recognized as one of these new human rights. Such multiplication contributes to a 'demonetarization' of the authentic Human Rights. I take the example of Intellectual Property, recognized by the EU as a Human Right and thus placed on the same level as Privacy, and which arbitrates between DP and privacy as human rights. Can we soon imagine conflicts between DP and Privacy? I am sure it might be the case, if we imagine a radical distinction between these two rights, considering the first one in a more positive approach, limiting but also asserting the right of DC to process information, and the second one as constituting a negative approach, forbidding certain processing. I take only two examples: the right to remain anonymous and the right to be disconnected. To what extent should these two rights be enacted and under which conditions? The answer will be different according to these questions if we consider as separate the two faces of the same Human right? This possible conflict is an essential risk linked to the separation of the two Human rights and would contribute to a weakening of our liberties. What about the Data Protection Authority at the direct service of D.P. and only indirectly at the service of Privacy? We are convinced that DPA must be the Privacy watchdog and not only the Data Protection guardian.

Conclusions

DATA PROTECTION must not be considered as a fundamental human right but as a tool at the service of our self-development and should thus not be placed on the same footing as PRIVACY.

Data Protection is rather a consequence of the positive obligation of our democratic states to give an answer to the challenges our digital societies are creating in respect of our ability to become full citizens.

In that sense, DATA PROTECTION legislations are derived from PRIVACY as a human right. They must be adjusted or complemented according to the new challenges, our self-development at the service of our democracy as informed, free and capable of choices citizen, has to face in our digital environment.