How future-proof is the privacy/data protection connection?

VUB – International Workshop : *'Exploring the Privacy and Data Protection connection – Legal notions of Privacy and Data Protection in EU Law in a rapidly changing World'*, organized by Privacy Hub and LSTS, Brussels, May 14, 2019.

© Yves POULLET, Emeritus Professor at the Faculty of Law of Namur, Co-Chairman of NADI (UNamur), Associate Professor at UCLille and member of the Royal academy of Belgium

Dear Colleagues,

Due to time constraints, I will develop my thesis in 15 minutes[1].

As retired academic, I feel authorized to be a bit provocative before a 'Data Protection' (and no more '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, definitively, 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 including the negative right to forbid processing by others. But today, if I analyse the Strasbourg Court case law (notably, Pretty, Botta, Barbulescu Cases), Privacy concept has another dimension. It encompasses all the conditions public and private authorities have to guarantee, in order to ensure the self-development of human being 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 - I prefer- the right to self-development and encompasses in an evolving way all the conditions, which reasonably might be needed for an individual within a determined society in order to '*build up his or her own identity*'. So, Privacy means in the same time both the right to be let alone and the right to act positively within the society freely by mastering his or her informational environment. Right of seclusion and right of inclusion constitute two intertwined facets of the same fundamental rights. You never might imagine that a person might be able to self-develop if he or she has, in the same time, the possibility to feel free from his or her four walls and to circulate with a minimum of trust and control 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

[1] Most of the reflections developed here are elaborated more fully in the book published recently: Y POULLET, *La vie privée à l'heure du numérique – Essai,* Collection des cahiers du CRIDS, n° 45, Larcier, Brussels, 2019,185 pages.

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 relationship to his or her data[2] at the detriment of the public interest.. I take only one example: your car insurer is proposing you that your premium will be fixed according to your driving real 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 in the same it puts into question the 'risk pooling' principle, principle which is fundamental in the insurance sector and thus to create prejudice to other people, candidates to the same insurance and the public interest.

So, when you are speaking about connection or complementarity between DP and Privacy, I prefer to speak 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 certain moment of the technological development. Taking fully into account the Privacy requirements facing the risks linked with our present and future technological developments, it would be important, at my opinion, to design new generations of privacy legislation or at least new avenues for interpreting data protection legal provisions. GDPR, with all the qualities we might recognize it, is only a point of departure at a certain moment of the technological development and not the holy Bible

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. 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?
      - 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 by personal data clearly is not sufficient at a time where big data are using both anonymous data and not anonymous data and where the distinction between both categories is flawed and flawed.
      - How to ensure the transparency of the 'logic when we are using '*deep learning AI systems',* based on random correlations'?
      - Sensitive data, as Cambridge Analytica revealed it, have to be considered not *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 to enlarge considerably 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 just enacted, discussion about the so-called 'gratuitous' Digital content services: and the problem of their effective use of 'counter-performance' by consumers

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

through the provision to Data Controllers of their data has clearly revealed the difficulty to apply GDPR 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 number of DP specialists, it is far to be simple to solve questions raised by blockchain applications in the context of GDPR. How to ensure within blockchain context, the right to delete or to correct my personal data? How 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 GDPR application. So, 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. So, might be pointed out the problems of discrimination as regards the access to new health services linked with the new technologies, the problem of the future of our mankind, the limits of our possibilities to determine the genetic baggage of our progeniture.

3. **What do we need in the future?** These examples show very clearly that definitively we have to go far beyond Data Protection provisions, if we want to address correctly the challenges tomorrow we will face 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 constitute from now on the driven 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 datification of our lives… we never can 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 a mental privacy to be protected)
   - 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 AI and more generally about all Information systems
   - 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 - I am of opinion that this question will become a major problem due to the AI possibilities of prediction and of discrimination, due to 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 principle of precaution (Digital environment) when we face to a disruptive innovation like blockchain, intelligent cars, AI,…

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 to set up a system of evaluation and control including by DPA, in order to decide then on a more permanent basis

SELF DEVELOPMENT AND DIGNITY must be the KEYWORDS in the future and that 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 have to joint together for that reflection. Only by our common and coordinated efforts, we will help people and society 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 assisting to a multiplication of human rights, the recognizance of D.P. as a human right is one of these new human rights. That multiplication contributes to a 'demonetarization' of the authentic Human Rights. I take the example of Intellectual Property recognized by EU as a Human Right and thus is placed on the same level than Privacy and makes necessary the arbitration between these two Human rights. Can we imagine tomorrow 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 as 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, these two rights ought to be enacted and at 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?

5. **Conclusions -** I come to the conclusions

   - DATA PROTECTION definitively must be considered not as a fundamental human right but as a tool at the service of our self-development, and thus not 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 society are creating for our capabilities to become full citizens.

   - In that sense, DATA PROTECTION legislations are derived from PRIVACY 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.