EJPLT

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Data Protection and vulnerability

PASQUALE STANZIONE
President of the Italian Data Protection Authority

Abstract

This contribution describes the evolution of the right to privacy from the traditional right to be let alone to data protection, enshrined as an autonomous right in the Charter of Fundamental Rights of the European Union. While illustrating the most innovative features of this right, the author also emphasizes that data protection represents an essential guarantee for freedom, equality and dignity with respect to vulnerabilities: both traditional ones and those induced by new technologies.

Keywords: data protection - dignity - equality - habeas data - identity – labeling - new technologies - right to be let alone - vulnerability.

The title of my speech underlines an essential idea: the awareness of how today new technologies expose us to new vulnerabilities and amplify the more 'traditional ones'.

If in the early twentieth century the 'domain of technology' was considered a distinctive feature of the post-modern age, it characterizes, even more, our times, in which technology risks losing its instrumental nature to become an aim in itself, making a human being no more its dominus but subordinate to itself. This happens essentially for an intrinsic characteristic of new technologies: the transforming power, the ability to develop new meanings of the reality.

The news hierarchy decided by algorithms, the selective power of indexing that shows only some contents and not others, are a paradigmatic example of how new technologies condition the very formative process of our beliefs, shaping public opinion and undermining the individual self-determination.

So it's up to the law to restore that human being centrality, which alone is a guarantee of a harmonious relationship with the technology and, at the same time, consolidates the personalist approach on which our Constitution and the EU system are based, whose activities place the individual at their heart, as stated by the preamble of the Charter of Fundamental Rights of the European Union.

This approach - both progressive, democratic and personalist -has made it possible to govern the relationship between individual and technology according to the evolution of the right to privacy in Europe in all its complexity, from traditional right to be let alone to data protection. As stated by the Council of Europe Convention n.108/1981, this right has to be read as a protection of individuals with regard to automatic processing of personal data. Data protection will acquire 'constitutional' rank with the Charter of Fundamental Rights of the European Union, as *habeas data:* equivalent, in the digital society, of what *habeas corpus* has represented since the Magna Carta; as the main prerequisite of immunity from power, it is promoted by the State, the market or technology.

Significant was the assonance with the Riley v. California ruling of 2014, by which the American Supreme Court extended the traditional guarantees provided for measures restricting personal freedom to the search of cell phones. The connection established between physicality and the electronic body is here much more than symbolic: the traditional guarantees granted to the h*abeas corpus* are extended to *habeas*

data, according to that evolutionary line that has made privacy a prerequisite of freedom and democracy together.

In Europe, however, the path of privacy has also marked an essential turning key in terms of values, emancipating this right from the dominical dimension of traditional bourgeois prerogative (right to be let alone), in order to assert itself as a means of protecting the socially weaker fringes from the abuse of a power that is primarily informative. This 'enrichment' of the original nucleus of the right with more modern demands was made possible by the conjunction, borrowed from the European system, of the American idea of constitutional privacy with the more continental one of guaranteeing social dignity.

Thus, on the one hand, the idea of informative self-determination has developed as a new expression of freedom of the individual in the construction of his/her own identity.

On the other hand, in its not only recent evolution, privacy has developed in all its potentiality the component linked to dignity, enshrined by the post-war Constitutions and, in particular, by those (Italian and especially German) of the countries where totalitarian regimes had carried out the worst violations of the 'right to have rights'.

This idea would have deeply permeated the jurisprudential, but also the legislative reading of data protection, according to a line that from the guarantees of freedom of the worker established by the 1970 Statute, would then have reached the anti-discrimination component of privacy, as a factor of protection of minorities or individuals particularly vulnerable to risks of stigmatization.

With the introduction of a dynamic protection, with a strong publicistic vocation, also based on the powers of intervention and control of the data subject, what had traditionally been conceived as *jus solitudinis*, intangibility of the private sphere from undue external interference, has thus been enriched with a new content and, in comparison with a reality so deeply affected by new technologies, has become a pre-condition for equality and for the exercise of fundamental rights.

In this sense, the right to data protection develops, to the end, the American idea of privacy as freedom of self-determination, a counter-majoritarian defence 'of the undecidable' sphere from primarily State interference, which has allowed, for example, in the USA, the right to contraception and abortion to be rooted on the Fourth and Fifth amendments (Griswold vs. Connecticut 1965, Roe vs. Wade , 1973), and in Europe on art. 8 ECHR to envisage the right to death with dignity [(Pretty v. UK 2002], to make use of assisted procreation (Costa and Pavan v. Italy, 2012) or the right of the born to seek their own origins, although compatible with the choice of maternal anonymity (Godelli v. Italy, 2012).

However, in the European reading, the dignity component has also made it possible to develop the social dimension of privacy (increasingly characterized, in the meantime, as protection of the individual with regard to the processing of his/her data) as the right to freely live out one's individuality also in the social dimension, protected from discriminatory risks or social stigmatization (ECtHR, Delfi AS v. Estonia, Sidabras v. Lithuania, 2015).

For this reason, since Convention 108 and, shortly afterwards, with the directive 95/46, enhanced protection has been granted to sensitive data (and in particular to those expressing an associative choice), demonstrating that privacy, far from encouraging isolation, is instead functional to freely establish strong social ties and also, where appropriate, connoted from an ideal point of view. Sensitive data were and are protected, in fact, to guarantee not their secrecy but their maximum public disclosure, without thereby exposing the data subject to discrimination. The anti-discrimination function of data protection (and,

above all, of sensitive data) would then prove, in the years to come, to be an extraordinary guarantee of equality, in a society increasingly prone to labelling.

It is significant, in this sense, that the Court of Cassation, in the case of sick children, has decided to extend the enhanced protection granted to their health data to their parents as well, because of the discriminatory potential related to information on the condition of discomfort and particular vulnerability, typical of those who are burdened with the care of children suffering from diseases (Cass., n. 16816/2018).

As is also relevant the expected subtraction of the disclosure obligations of data relating to grants, from which the socio-economic condition of the beneficiary can be inferred (Article 26, paragraph 4, Legislative Decree 33/2013).

This anti-discrimination vocation has represented the center of gravity around which the gradual transition from traditional privacy to data protection has emerged, progressively establishing itself as a constituent element of a new form of citizenship able to strengthen the conditions for citizens' participation in collective life, thus favouring sociality also -and above all- for those who would have feared its repercussions on the individual sphere, because of their own subjective conditions. Therefore - according to the scheme for which '*remedies precede rights*' - that fundamental passage 'from secrecy to control' was outlined, made possible also by a jurisprudence of the European Court of Justice that emphasized the properly constitutional dimension of this right.

Despite the protection of data was born, in fact, as functional to the development of the internal market, the scope of the directive has gradually reversed the terms of the relationship**,** enhancing the protection of that right 'to freedom' which, according to the Court, should be given precedence over the mere interest of controllers to increased profits (C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [2014]). And if in this case the Court has recognized a real *Drittwirkung* to the right to data protection, with regard to a private subject such as Google, elsewhere it has gone so far as to establish the direct applicability of the proportionality principle (C-139/01 *Österreichischer Rundfunk and Others* [2003].). A strong reading of this principle - heterointegrative of reasonableness principle – has allowed our Constitutional Court to outline a democratically sustainable balance with respect to the relationship between data protection and administrative transparency (Const. Court, n. 20 of 2019). Thanks to the reconsideration, in a personalist key, of this relationship, it has in fact been possible to bring the discipline of administrative transparency back to its democratic function of 'governing public affairs in public', counteracting the paradoxical effect of opacity from information excess, due to the unreasonable extension of publicity obligations.

But the social function of data protection has also proved to be decisive with respect to the 'structural', almost ontological vulnerability that characterizes the position of the individual about the increasingly pervasive private powers, exercised with the pretension of inscribing the code of life and society in the general contract conditions.

Here I'm using the term 'vulnerability' in the meaning in which it can be connected, for example, also to the consumer, that is to say with reference to general categories connoted due not so much to specific subjective as to relational characteristics, i.e. derived from the relationship in whose context they are considered. Here lies the transition from the abstract, 'disembodied' subject, to the person, in the peculiarity of his/her condition (*homme situé*).

Precisely this passage has allowed a new approach to vulnerability, which is a paradoxical notion, because it is both a prerequisite and an effect of human autonomy. But it is also a complex notion , because it is universal - all human beings are vulnerable -

individual - since it does not affect all people in the same way -; potential - possible, but not certain realization of a risk -; relational and contextual - we are vulnerable in a given context: moreover, it is society that makes individuals vulnerable, not the contrary -; finally, reversible - and in fact with appropriate individual and social measures it is possible to reverse this condition.

On the basis of these elements, we can outline a basic notion of 'vulnerability' as a common connotation of the human condition (a sign of existence, for Simon Weil), next to which it can be seen the variability of the situations in which it is declined: conditions due to age, gender, health and other discriminating factors. One of these conditions may, however, also be the relationship, legal and socio-economic, structurally asymmetrical, of which the subject is a weak part: so for the consumer or the user of digital platforms.

Concerning the latter subjective category, data protection discipline offers some decisive guarantees to rebalance its conditions of vulnerability, at least partially curbing the irresponsible power of web titans.

Through the application - possible, under the GDPR, without further requirements - of the European law to extra-European controllers, it has in fact been possible to impose limits on the irrepressible collection of data, assimilated to mere currency to be deducted in contract, with the risk of monetization of privacy, which today represents the real democratic issue.

On this ground, the Italian Data Protection Authority has promoted a debate within the European Data Protection Board, in the awareness of how this issue represents an essential matter in the evolution of data protection law. On the one hand, in fact, the *zero price economy* has made the 'services versus data' negotiation scheme an ordinary practice; on the other hand, admitting the possibility of remuneration for consent risks leading to the creation of digital sub-proletariat, i.e. social strata likely to surrender, with their data, the essential core of their freedom.

On this 'slippery slope' is at stake, perhaps more than in any other field, the European identity as a 'Community of law' founded on the synergy between freedom, dignity, equality, as essential safeguards that no reason of State or, much less, the market can violate. And in this sense, data protection may represent an extraordinary barrier to the risk of refeudalization of social relations and reconstitution of census-type discrimination even among users of the internet, whose inclusive and democratic vocation risks succumbing under the weight of surveillance capitalism.

With respect to the condition of particular vulnerability of the minor, then, the Italian legislator has given the Italian Data Protection Authority a central role in the fight against cyberbullying, assigning him the power to decide on instances for the removal of illegal/harmful content. This is a forward-looking provision, aware of how children today can represent the elective 'victims', at the hands of their own peers, of a misuse of the internet, where their fragility is amplified also due to the reduced perception of the terribly concrete impact of every gesture, of every word, every image posted on social networks.

But the context in which data protection can represent a fundamental defence for the individual with regard to new and subtle forms of discrimination is that of artificial intelligence and algorithmic decision making, to which decisive and far from neutral choices are increasingly being delegated, for private and public life: from medical diagnosis to 'predictive' police, from the assignment of teaching locations even to the assessment of the adoptive suitability of couples (as in Florida).

Moreover, not even what has traditionally been considered the last bastion of human assessment, namely judicial (in particular criminal) process, seems immune from the

tendency to mechanize decisions, with effects often much more discriminatory than those of the worst human decision.

An algorithm used in some American courts for the prognosis of criminal recidivism has been proved, for example, inclined to grant a higher score to African-Americans, of course in the absence of any criminological reason, but only on the basis of the statistics taken as a reference photographing a penitentiary and judicial condition not really representative of the phenomenon.

The result to be drawn from the use of technologies that should ensure maximum impartiality is likely then to be, paradoxically, more discriminatory than the " human, too human 'rationality', at least whenever the algorithms reflect the pre-comprehensions of those who design them or are 'trained' with data that are not representative of actual reality, in all its complexity.

From this point of view, both the GDPR and the law enforcement directive (n. 2016/680) provide some essential guarantees which are increasingly being used in case law to establish an embryonic legal status for artificial intelligence.

In fact, not only does the Regulation subject the admissibility of fully automated decisions based on 'special categories' of personal data to particularly restrictive conditions, but in any case recognizes the right to an explanation of the underlying logic, to challenge it and to obtain human intervention in the automated process, precisely to correct any *bia*s that might otherwise produce detrimental effects.

These reinforced obligations of algorithmic transparency are, however, particularly relevant precisely because they allow to overcome, at least in part, the opacity of such processings, which really makes such decision-making processes the new *arcana. imperii.*

A further guarantee of a preventive nature then derives from the necessary subjection of automated decisions to impact-privacy assessments: an institution which, precisely because of its effectiveness, has been proposed to enhance in a broader perspective, allowing the assessment of similar processings' impact not only on data protection but, more generally, on rights and freedoms, given the natural interrelation between data protection, dignity and other fundamental rights. Widening its spectrum, the impact assessment would become a PESIA: privacy, ethical and social impact assessment*:* a prognosis of the ethical and societal impact of processing, conducted according to the parameters of respect for fundamental rights and anti-discrimination protection as well as the right to data protection.

The requirements set out in the GDPR were enhanced by the Council of State which, in the case of teachers' algorithm, considered the software to be a 'digital administrative act', to be subject to full jurisdiction guarantees according to an 'enhanced declination of the transparency principle ', as well as to the prohibition of the exclusive algorithmic decision and to the equality and non-discrimination principle.

The risk of discriminatory use of algorithmic decisions, all the more so if functional to the exercise of coercive power is, moreover, the subject of particular attention under Directive 2016/680 and Legislative Decree 51/18 that transposed it. If, in fact, the former has enshrined an express prohibition of automated decisions based on special categories of data, which induce discrimination, the latter has been granted criminal protection, in an aggravated form, in awareness of the risk of a combination of investigative power and the increasingly strong one of technology, especially for the most vulnerable subjects.

The racial profiling sometimes practiced in the aftermath of September 11th. by law enforcement officials, targeting individuals for suspicion of crime based on the individual's race, ethnicity, religion or national origin, comes to mind. If these pre-comprehensions are added to the computing power, the pervasiveness of digital investigations and the profiling capacity of the algorithms, the risk of further deeper and more subtle discrimination against

minorities or of those perceived as 'different' is greatly aggravated.

It is no coincidence that the European Union is investing a great deal of its identity building in this area, also in its relationship with the USA, as well as demonstrated by Schrems jurisprudence and the personalist vocation already underlying the Ventotene manifesto is taking on new horizons.

As President of the Italian Data Protection Authority, at the beginning of a mandate that will go on for important years, I can already indicate, as a priority objective, the protection of vulnerable subjects such as minors, migrants, sick people, inmates in prison, or in any case belonging to minorities; of all those whose fragility - by nature or circumstance - risks making them really 'naked' in the face of power.

It is precisely on this very delicate ground that data protection will express its profound sense, as a precondition of any other right or freedom; a prerequisite for a society of dignity.