THE FUTURE OF DATA PROTECTION IN THE NEW EU DIGITAL SCENARIO

Professor Pasquale Stanzione – President of the Italian Data Protection Authority

I would like to thank my friend Prof. Zeno Zencovich for inviting us to discuss such an important issue as the future of the Data Protection Authorities, which has come at a very important time.

On the one hand, in fact, this year marks the 25th anniversary of the establishment of the Garante: one could not imagine a more fruitful moment to discuss, together, the roots and the future of this Authority (also in comparison, precisely, with its European counterparts). On the other hand, the punctuality of the solicitation refers to the European regulatory and legal context, which has been characterised for about a year by the centrality of the legislative initiative on the topic of digital and its governance, with direct reflections on the discipline of data protection. The Digital Services Act, the Digital Markets Act, the Artificial Intelligence Act, the Data Governance Act, the directive on platform work, and the regulation on political targeting: these are just a few, albeit the main ones, of the regulatory acts proposed by the Commission on this subject, which, besides extending the competences of the Data Protection Authorities to a not insignificant extent, significantly borrow many of the central institutes of the GDPR. They therefore represent, in a certain sense, the confirmation of how the Regulation has represented an avant-garde legislation, destined not only to assert itself beyond the European borders (as demonstrated by the Chinese, Brazilian, and Californian cases) but, above all, to become a paradigm for subsequent interventions.

In short, the essential features of the Regulation are its far-sightedness (also due to its technological neutrality) and flexibility, which have been its real strengths to the extent that they have made it attractive. Thanks to an appropriate combination of rules and principles, rigour and flexibility, this discipline, in the continuum between the directive and the new European legal framework, has in fact enabled data protection to best perform the social function that would later be unequivocally assigned to it by Recital 4 of the GDPR. Constantly balanced with the most diverse individual and collective needs, this right of freedom (as indirectly described by the EU Charter of Fundamental Rights) has revealed its own strength in its 'mildness', i.e., in its never being a tyrant and in being able to strike the best balance with the legal interests at stake.

And if data protection has always proved to be an unavoidable prerequisite for freedom, equality and dignity, more recently it is proving, in an increasingly unequivocal manner, to be an essential democratic guarantee, the centre of gravity of the relationship between private and public, personal and political, rule of technology and rule of law.

Last but not least, thanks to the choices made with regard to the limitations of individual rights in order to fight the pandemic, Europe has shown, precisely in the field of privacy, that it is able to combine freedom and solidarity without opposing them, avoiding the technocratic shortcuts of bio-surveillance. Faced with a technique that has proved capable of pushing the forms of control beyond all limits, the data protection discipline, throughout its evolution, has provided the tools to place it truly at the 'service of person', promoting social sustainability and

becoming the interpreter of the anthropocentric direction that Europe intends to give to innovation. Therein lies the farsightedness and resilience of the data protection discipline: **having grasped the 'Zeitgeist'** in its deepest roots and in all its evolutionary capacity.

The *Garante* has guided this process by changing its very nature, adapting its action to emerging social needs and to the protection requirements expressed by citizens, as an Authority guaranteeing a fundamental right exposed, more than others, to the dynamism of the relationship with technology.

And if this flexibility of action has been imposed in the passage from the directive to the regulation, it will be even more so in the present and in the years to come, when the speed and importance of technological evolution is and will be such as to undermine consolidated structures and reference coordinates, even though they are considered constant. The legislative proposals put forward by the EU Commission last year already imply a significant change in the role of the Data Protection Authorities. Whether a specific role is attributed to them (as, for instance, the recent proposals for regulations on political targeting and platform work do) or not, the impact of new regulatory forms on data protection matters has, in fact, inevitable repercussions also on the functions of the DPAs. And the very change in digital governance that each of these proposals envisages entails, moreover, the need not to subtract areas of protection of data protection rights from their own Authority, with all the guarantees, first and foremost of independence, that characterise it.

This is an issue we have explicitly raised before Parliament in the various hearings held in the run-up to the DSA, DMA and, more recently, the Artificial Intelligence Act (AIA) proposals.

In the case of the DSA and of the DMA, it has been noted, in fact, how the affinity of the regulatory model between the GDPR and the DSA should suggest the valorisation of the experience acquired by the Authorities of data protection, also conferring on them the role of Digital Service Coordinator (DSC). The **identification of the DSC in bodies of such competence, transversal** and with a strong vocation to the protection of fundamental rights, would contribute to a greater coherence and effectiveness of the multi-level system of governance provided by the DSA.

As we have suggested to the Chambers, a similar solution should be envisaged for the IA regulation. In spite of the fact that many of the activities being regulated affect fundamental rights, the list of subjects indicated in the *draft* as having supervisory powers is not limited to independent administrative authorities.

This is a not insignificant aspect, insofar as it leads to a substantial weakening of the guarantees of fundamental rights and, in particular, of the right to the protection of personal data, the effective protection of which is based (Articles 8 TFEU and 16 TFEU) on the supervision of independent authorities.

Insofar as the regulation of the AI affects the guarantees of the processing of personal data, the lack of involvement of the Data Protection Authorities results in the removal of their competences. In view of the close interrelation between AI and privacy and the characteristics of independence that characterize the statute of these Authorities, it would be useful to think

about the solution proposed by the Edps and the Edpb, aimed at suggesting the attribution to them of the role of supervisory authority for AI.

This solution would also guarantee a considerable simplification for users, who would have to address a single authority for AI systems operating on personal data, greater consistency of the overall discipline considered, as well as the extension of the status of guarantees (also in terms of independence) of the Data Protection Authorities to the AI sector.

The Data Protection Authorities (and the Italian Garante, of course, no less) already possess the necessary competence and, at the same time, independence to ensure a fully consistent implementation of the regulation and a forward-looking application of its provisions.

Even if, however, the DPAs were not to be specifically designated as supervisory authorities in relation to the DSA and AIA, as we had hoped, the indisputable fact remains that their powers have been extended by the new obligations introduced and the need to ensure compliance with them.

A similar extension of the competences of the DPAs will result from the regulation on political targeting and from the directive on platform work, both of which assign them specific supervisory powers on the compliance with the requirements introduced. On the whole, therefore, this is not a mere summation of new tasks and powers, **but a real progression in the path, already under way, of mutation of these Authorities, from guarantors of (only) privacy to Guarantors of the person in the digital reality** (rather than only of the 'digital rights' of the person, as also assumed in Parliament).

The sense of this path is emblematically traced by an **amendment to the European delegation law, which assigns to the Garante the competence of national authority for human rights**, grasping the reality of the right to data protection today, which is increasingly characterised by being not only a fundamental right in itself, but also a **prerequisite for the exercise of any other right and freedom.**

The ontologically transversal nature of the right to data protection (which, as a fundamental right under Art. 8 of the European Convention on Human Rights, is not a mere right of citizenship), and consequently also of the activity of the Garante, is, in fact, the real strength of this solution. The Garante is the authority appointed to protect the individual sphere from undue interference by unfair commercial activities, invasive online profiling or digital stalking by large platforms. It is the body from which to request protection against the unscrupulous use of micro-targeting, aimed at conditioning behaviour and choices, not only in terms of consumption (as demonstrated by the Cambridge Analytica case). The Garante is the Authority entrusted with the task of ensuring that the legitimate exercise of the right to (and to) information does not degenerate into media pillorying or keyhole watching, thus violating individual dignity and privacy. It is the Authority before which everyone can exercise his or her right to be forgotten with respect to the risk of a distortive use of the network and its 'eternal memory'.

Today, minors (if over 14 years old, also independently) can turn to the Garante to obtain protection against injuries to their dignity caused by cyberbullying, revenge porn, hate speech, etc. In addition, a bill was approved at first reading, which gives the Garante the power to decide

on requests - submitted by minors, if over 14 years old, also independently - for the removal of content inciting to suicide.

The Garante is confronted on a daily basis with the danger that the digital transformation of the economy may degenerate into the monetisation of freedom, with the risk of a real re-feudalisation of social relations. The Garante has also been confronted with the 'digital caporalato' to which an uncontrolled drift of the gig economy risks leading. The Authority has had to evaluate, on several occasions, the legitimacy of the recourse to particularly invasive investigative techniques, such as those based on facial recognition, providing indications for a correct balance between the dignity and liberty of the person and the needs of crime prevention. Moreover, the Garante is constantly confronted with the challenges that algocracy poses to fundamental rights and freedoms if it is not guided by an anthropocentric approach, and with the risk that algorithms (which could reduce inequalities and promote equality) may lead to new forms of discrimination.

The Garante is, therefore, today, an Authority delegated to the protection of the person, of his rights and liberties with respect to the vulnerabilities amplified or induced by the new technologies. Insofar as the freedoms and rights are exercised, today, to a substantial extent (if not even prevalent) on-line or, however, in forms and ways strongly conditioned by the new technologies, a right - such as that of the protection of data - which allows an anthropocentric and democratically sustainable government of the technology, cannot but represent, in fact, the inescapable prerequisite for the guarantee of such rights.

What would become of the right to self-determination in matters of health, procreation and existence if we could not guarantee confidentiality on essential choices such as vaccination, end-of-life and abortion? And how can pluralism and freedom in political and electoral matters be guaranteed if the very contents offered by the network are pre-selected and modelled on the type of voter attributed to the individual by the algorithm? How can we guarantee that i.a. does not evoke, and even deepen, the preconceptions from which it is supposed to free us, in the absence of effective control over the data with which to train the algorithm (think of the Loomis case)?

These are just some of the possible examples to illustrate, albeit without a detailed taxonomy, how the right to data protection today represents the necessary condition for the effectiveness of the guarantee of fundamental rights.

This is why the Garante, in protecting the right to the protection of personal data, inevitably also ends up protecting fundamental rights with a wide-ranging action, due to the transversal nature of the competences entrusted to him. I believe that the increasingly close interrelation between data protection and fundamental rights will be the way forward for the Data Protection Authorities in the near future.