Ginevra Cerrina Feroni[*]

Governing Artificial Intelligence through Data Protection: The Strategic Role of Independent Authorities in the Age of Algorithmic Power[**]

Artificial Intelligence (AI) represents not only a technological shift but also a constitutional challenge. As AI systems become more involved in social, economic and legal decisions, the role of Data Protection Authorities (DPAs) is becoming increasingly important. This short essay, based on the speech held by the Vice President of the Italian Data Protection Authority, Prof. Cerrina Feroni at the 33rd European Conference of Data Protection Authorities, examines the structural interdependence between AI and personal data, placing data protection at the core of AI governance. Drawing from the experience of the Italian DPA and comparative international examples, it analyses four critical areas: legal bases, data transfers, automated decision-making, and protection of vulnerable individuals, where DPAs are establishing the normative boundaries of AI systems. It further suggests that DPA's role might benefit from evolution from reactive enforcers to proactive institutional actors engaged in system design, audit, and risk classification. This essay tentatively suggests that the legitimacy, legal certainty, and democratic accountability of AI governance may be best served by the central involvement of independent supervisory authorities.

Keywords: Artificial Intelligence, Data Protection, Independent Authorities, GDPR, AI Governance, Algorithmic Accountability.

[*] Vice President of the Italian Data Protection Authority; Full Professor of Italian and Comparative Constitutional Law at the Faculty of Law of the University of Florence; Lawyer enrolled in the Special Register of University Professors; Member of the Board of the Italian Association of Comparative Public Law; Member of the Board of the Italian Association of Constitutionalists.

[**] The paper is the text of a keynote speech presented at the 33rd European Conference of Personal Data Protection Authorities ("Spring Conference"), hosted by the Personal Data Protection Service and held in Batumi. The information and views set out in this article are those of the author and do not necessarily reflect the official opinion of the European Commission.

1. Introduction

It is fair to say that the field of Artificial Intelligence (AI) is having a significant impact on governance, institutional accountability, and fundamental rights protection. It is not a self-contained phenomenon, but rather a transformation that can be seen across public administration, private markets, and daily social interactions. It is interesting to note that a key distinguishing feature of AI, as opposed to previous technological advancements, is its capacity to make or influence decisions independently. Decisions that were once exclusively within the domain of human judgment and institutional procedures are now being influenced by AI. This reallocation of decision-making authority from humans to machines may entail a significant shift in how accountability, transparency, and rights are operationalised.

Moreover, the general-purpose nature of AI means that it has the potential to affect a wide range of regulatory domains, including consumer protection, labour law, media law, criminal justice and health governance. It is important to note that the way in which legal regimes intersect with one another can create zones of normative uncertainty, which has the potential to complicate the regulatory landscape. In such an environment, it may be that treating data protection as a sectoral concern is no longer sufficient. Otherwise, it shall be seen as a cross-sectional structural safeguard for democratic societies.

As AI evolves from a tool of optimization into an architecture of decision-making, it may be helpful to consider who should define its limits. It would be interesting to know who is responsible for ensuring its accountability and who is there to defend individuals when the effects of algorithmic systems on their lives are not always clear.

In the European legal tradition, it is understood that the defence of fundamental rights against technological overreach is best served by institutional rights-based mechanisms. Among these, Data Protection Authorities (DPAs) hold a unique position. They are equipped with investigative, corrective, and advisory powers, and are mandated to safeguard the rights enshrined in the Regulation (EU) 679/2016 (GDPR).

However, it is important to acknowledge that their role in the governance of AI systems is still evolving and, at times, contested. This essay aims to shed light on the importance of DPAs in shaping lawful, rights-compatible AI.

Drawing from practical enforcement experiences, legal doctrine, and comparative oversight practices, the following sections humbly suggest a proactive, interdisciplinary, and anticipatory model of data protection in the age of AI.

2. Artificial Intelligence and the Imperative of Data Protection

The relationship between AI and personal data is not incidental, but constitutive. It is fair to say that most advanced AI models, from generative systems to predictive analytics, are trained, refined, and deployed using data that describes or relates to individuals. No matter what form it takes, whether it be user prompts, sensor data or behavioural profiles, there are significant legal implications to consider.

Under the GDPR, personal data processing is permissible only under specific legal bases.[1] In the context of AI, particularly in the area of model training, consent and legitimate interest are often cited as the more relevant ones. However, it is important to acknowledge that both of these approaches have their challenges.

To be valid, consent must be informed, specific, freely given, and revocable. In opaque, large-scale training operations, meeting these criteria can sometimes be challenging.

On the other hand, legitimate interest requires a balancing test: this involves an assessment of whether the interests of the controller override the rights and freedoms of the data subject. In the field of AI, where risks can be intricate, cumulative, and challenging to anticipate, such evaluations necessitate a high degree of scrutiny.

Furthermore, cross-border data flows give rise to a number of additional challenges. It is important to note that AI developers often distribute computational tasks across jurisdictions, sometimes involving third countries without adequate legal safeguards. Even if Chapter V of the GDPR imposes strict conditions for such transfers, the process of enforcement can be hindered by a lack of transparency. Indeed, many developers may not disclose the location of data processing or storage, citing reasons such as trade secrets or technological complexity.

Finally, article 22 of the GDPR seeks to ensure that decisions made solely through automated processing do not have legal or similarly significant effects. Exceptions do exist, but they are subject to procedural guarantees, including the provision of meaningful information, the right to contest, and the involvement of human oversight.[2]

[1] See, in particular, articles 6 and 9 of the GDPR. While Article 6 outlines the general lawful bases for processing any personal data, Article 9 focuses specifically on the processing of special categories of personal data, which is more restricted.

[2] Article 22 of the GDPR states that:

"1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

In this context, DPAs have begun to investigate and to initiate administrative proceedings that, in some cases, led to the imposition of fines. In Italy, the enforcement actions taken by the Italian Data Protection Authority (Garante) against Replika and ChatGPT have underscored the pressing need for urgent action, particularly in light of the absence of legal bases, the need for greater transparency, and the crucial importance of protecting minors. Similar interventions by Canada[3], South Korea[4], and Japan[5] confirm the global relevance of these concerns.

3. The Democratic Value of Independent Oversight

The governance of AI is not a neutral, technocratic exercise, but an area of contested power. AI systems influence behaviour, shape narratives, and generate knowledge and, moreover, have, in several cases, the potential to decide whether to guarantee or not the access to a range of services, including credit, employment, health, and public services. In this sense, the rules governing their operation and functioning are inherently political.

For this reason, DPA's role is not just about compliance. They are constitutional institutions with legal powers, technical competence and independence.

In this landscape, the institutional independence of DPAs is considered to be a democratic safeguard. Article 52 of the GDPR states that DPAs shall act with complete autonomy and independence, free from external influence. This independence should allow them to resist political and economic pressures, particularly in cases involving powerful multinational technology providers.

c) is based on the data subject's explicit consent

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision. […]"

[3] On 4 April 2023, the Office of the Privacy Commissioner of Canada (OPC) announced an investigation into OpenAI. This followed a complaint regarding the collection and disclosure of personal data without consent. More information available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/.

[4] On 17 February 2025, South Korea's Personal Information Protection Commission (PIPC) announced that DeepSeek had suspended its app-based service in Korea in order to comply with the Personal Information Protection Act (PIPA). This followed an inquiry and technical evaluation by the PIPC, which revealed a lack of transparency in DeepSeek's privacy policy and un-notified third-party data transfers. More information available at:
https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2784#none.

[5] On 3 February 2025, Japan's Personal Information Protection Commission (PPC) published detailed information regarding Hangzhou DeepSeek Artificial Intelligence's privacy policy, shedding light on how the company collects, processes and protects user data. More information available at: https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/.

Experience has confirmed the value of this model. The Garante's investigation into ChatGPT[6], which led to a temporary restriction on processing, several corrective measures and a fine, was carried out independently, but in dialogue with European counterparts and civil society. It demonstrated that fundamental rights could be upheld even in cases that were moving quickly and receiving a lot of attention.

However, it shall be ensured that institutional independence is commensurate with institutional capacity. Effective oversight necessitates legal certainty, technical expertise and operational resources. In fact, DPA personnel must be equipped to not only respond to complaints, but also to conduct audits, interpret complex algorithmic systems, and engage in strategic foresight. Such institutional capacity, together with the independence requirement, aims to guarantee that DPAs are able to anticipate or intervene promptly on technological trends.

4. From Ex Post to Ex Ante: Redesigning the Supervisory Model

It is clear that the traditional regulatory model, based on ex post enforcement, is not always suitable when faced with the rapid pace, vast scale and intricate nature of AI. Intervening before harms occur is advisable, as this will render oversight more effective. A new supervisory paradigm shall be considered: a paradigm that combines ex post powers with ex ante engagement.

This change means that authorities need to take a more active role in designing and using AI systems. As a matter of example, tools such as regulatory sandboxes help DPAs and developers work together to identify and reduce risk in a controlled environment. Early dialogue has the potential to reduce uncertainty and promote compliance by design.[7]

It is also vital that DPAs contribute to the definition of risk classification systems. This is essential to ensure that data protection principles are embedded in the very architecture of AI regulation. Furthermore, DPAs shall have access to the technical underpinnings of AI whenever technically possible: documentation, training data and

[6] The Garante's investigation revealed several breaches of the GDPR carried out by OpenAI, with regard to the processing of user personal data. These violations included: failure to ensure transparency and to provide users with the necessary information, a failure to implement adequate age verification safeguards, a potential exposure of minors under 13 to inappropriate content, a failure to notify the relevant parties of a cybersecurity breach, and a disregard of an earlier order to conduct an urgent informational campaign. More information available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432.

[7] For this reason, since 2021, the Italian Data Protection Authority has been a permanent member of the FinTech Coordination Committee, which was established by the Ministry of Economy and Finance. The Committee oversees regulatory sandbox initiatives designed to test innovative financial solutions, including those based on AI and data-driven technologies. The sandbox initiative has received 53 applications since the launch of the first application window. 13 of them have been accepted. More information are available at: https://www.dt.mef.gov.it/it/attivita_istituzionali/sistema_bancario_finanziario/fintech/index_bak.html.

algorithmic logic, as operational transparency is, of course, an essential component of this process.

Without access to these layers, enforcement will not achieve its full potential.

In these sense, algorithmic audits, conducted by interdisciplinary teams, are a key tool. It is possible that these audits may reveal not only legal non-compliance but also structural risks such as bias, discrimination, or a lack of contestability. The integration of such practices within the framework of AI governance systems has the potential to enable the verification of compliance. The objective is not to impose excessive regulation, but rather to establish legal clarity. Responsible innovation becomes easier when expectations are known in advance. In order to ensure the efficacy of such enforcement and oversight mechanisms, they must be embedded within a broader, coordinated approach to AI governance.

5. Coordinated Governance and Rights-Based Convergence

AI governance involves many different stakeholders, such as regulators, competition and consumer authorities and, obviously, DPAs. This is due to the intricate nature of AI that produces effects on numerous areas. These may present challenges in terms of inconsistency, potential risks of fragmentation and jurisdictional conflict.

Hence, in the spirit of constructive dialogue, efforts shall be made to ensure an efficient coordination that is grounded in rights, with a view to avoiding outcomes that may be detrimental to all.

This process requires the presence of formal mechanisms of inter-institutional collaboration. As a matter of example, permanent coordination platforms, joint working groups and shared risk registers could be a way to align regulatory strategies. It is perhaps worth considering whether DPA members should have a more central role on these platforms, rather than playing a peripheral consultant role.

At the international level, convergence initiatives such as those of the Spring Conference of DPAs, G7, The OECD (Organisation for Economic Co-operation and Development), and Council of Europe offer promising frameworks, having the potential to contribute to the articulation of shared standards and supervisory priorities.

6. Conclusion

Artificial Intelligence is having an impact on the power relations between individuals, institutions and markets. It has the potential to influence the way in which decisions are made, information circulates, and rights are exercised or denied. In this context, governing AI might be interpreted as a means of governing power.

Data Protection Authorities have a unique role in ensuring that governance respects legality, proportionality, and accountability. They bring together legal authority, technical expertise, and institutional independence.

Their role is not to hinder innovation, but rather to guide it within the confines of democratic principles. For this reason, they are not only regulators, but also constitutional guardians of fundamental rights.

In order to achieve this potential, it is necessary for DPAs to be fully integrated into AI governance frameworks, to consider expanding their mandate from reactive enforcement to proactive engagement and to equip them with adequate resources and legal tools.

Bibliography:

1. Italian Data Protection Authority, Comunicato Stampa - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro, 2023. <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432>.
2. Ministero dell'Economia e delle Finanze. Sistema bancario finanziario <https://www.dt.mef.gov.it/it/attivita_istituzionali/sistema_bancario_finanziario/fintech/index_bak.htm>l.
3. Office of the Privacy Commissioner of Canada, OPC launches investigation into ChatGPT, 2023. <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2023/an_230404/>.
4. Personal Information Protection Commission, Japan, Hangzhou DeepSeek Artificial Intelligence's privacy policy, 2025. <https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/>.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119.