Perspectives on the Application of GDPR Rules Regarding the Protection of Sensitive Personal Data in Romanian and European Practice

DR RAUL FELIX HODOŞ[1],
BUCHAREST UNIVERSITY OF ECONOMIC STUDIES, PHD CANDIDATE;
"1 DECEMBRIE 1918" UNIVERSITY OF ALBA IULIA, ASSOCIATE PROFESSOR, PHD

Abstract: *This article explores the normative, legal, and institutional dimensions of sensitive personal data protection within the European Union, with a particular focus on the application of* ***Article 9 of the General Data Protection Regulation (GDPR)****. Anchored in the principles of human dignity, equality, and proportionality, Article 9 represents a pivotal expression of European digital constitutionalism. Sensitive data are framed not as neutral informational inputs but as* ***moral constructs****, carrying the weight of identity, personhood, and social equality. Through doctrinal analysis and jurisprudential interpretation, the study traces how the GDPR transforms ethical values into enforceable legal obligations, including the* ***reversal of the burden of justification*** *for processing sensitive data.*
Keywords: *EU, GDPR, human rights, ethics, law*

The research further evaluates the expanding relevance of Article 9 in the context of **artificial intelligence**, where inferred sensitive data blur traditional legal categories. The **EU Artificial Intelligence Act (2024)** and the Ethics Guidelines for Trustworthy AI are examined as regulatory instruments that extend the GDPR's ethical architecture into high-risk algorithmic systems. Romania is used as a national case study, with analysis of the ANSPDCP's evolving enforcement role, highlighting both promising developments and structural limitations.

A comparative perspective contrasts the EU's rights-based approach with the United States' **sectoral, market-driven model**, emphasizing the originality and global influence of the European paradigm. The article concludes with a set of **policy proposals** focused on ethical-by-design mechanisms, institutional strengthening, and civic education. It argues that sustainable digital governance requires not only technical safeguards but a **cultural commitment to law as a form of ethical constraint**. The protection of sensitive data thus emerges as a cornerstone of democratic resilience in an age of accelerating digital inference.

Keywords: GDPR, Article 9, Sensitive Personal Data, Human Dignity, AI Regulation, Data Ethics, EU & Romanian Law, Digital Constitutionalism

The protection of sensitive personal data occupies a distinctive position within the European Union's legal and ethical framework. It is not merely a matter of procedural compliance, but an expression of fundamental values embedded in the constitutional fabric of the Union. The General Data Protection Regulation (GDPR), adopted in 2016 and enforced since 2018, marks a paradigmatic shift in the regulation of personal data, particularly with respect to what it defines under Article 9 as "special categories" of data. These include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life, or sexual orientation. The regulatory treatment of such data rests on a presumption of prohibition, subject to narrowly defined exceptions, which signals the seriousness with which the EU approaches informational harm and discrimination risks.[2]

[1] Dr Raul Felix Hodoş, Associate Professor, "1 Decembrie 1918" University, Alba Iulia, Romania and Ph.D. Student (his 2nd PhD) – The Bucharest University of Economic Studies Romania, and ORCID: 0000-0001-8500-135X, Scopus Author ID: 58563100400 , Web of Science Researcher ID ADG-7045-2022 Raul Felix Hodos – Google Scholar

[2] European Parliament and Council, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 9, OJ L119/1, 4 May 2016.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

This heightened protection stems from an underlying philosophical commitment to human dignity, as codified in Article 1 of the Charter of Fundamental Rights of the European Union, which asserts that human dignity is inviolable and must be respected and protected.[3] In this sense, the GDPR should be interpreted not only as a legislative instrument but also as a constitutional expression of European values. The linkage between data and dignity is particularly visible in the architecture of Article 9, where the obligation to justify any processing of sensitive data reverses the burden of proof. The data controller is no longer assumed to act lawfully by default; instead, they must demonstrate that processing is both necessary and proportionate in light of specific legal grounds.[4] This design choice reflects what scholars have described as "digital constitutionalism"—the embedding of ethical principles within the technological infrastructure of governance.[5]

The notion that data protection constitutes a form of moral boundary-setting is increasingly relevant in the age of algorithmic inference. With the growing capacity of artificial intelligence systems to extract sensitive attributes from seemingly benign data—such as predicting political orientation or health conditions from online behaviour—the traditional binary between sensitive and non-sensitive data has begun to collapse.[6] Such developments reinforce the importance of adopting a contextual and risk-based interpretation of sensitivity, as proposed by scholars such as Mantelero, who argues that the ethical justification for data regulation must now account for relational risks, not merely data categories.[7]

In response to these shifts, the European Union has introduced complementary regulatory tools, most notably the Artificial Intelligence Act, formally adopted in 2024. This instrument classifies AI systems that process biometric, genetic, or behavioural data as "high-risk," thereby triggering obligations of transparency, explainability, and human oversight.[8] The Act can be understood as extending the logic of Article 9 GDPR into the algorithmic domain, translating abstract human rights values into legally enforceable technical safeguards. This legislative direction has been reinforced by the "Ethics Guidelines for Trustworthy AI," published in 2019 by the High-Level Expert Group on Artificial Intelligence, which assert that AI must not only be lawful but also ethical and robust.[9]

Romania's implementation of Article 9 GDPR provides a concrete illustration of how these abstract commitments can be translated into national enforcement. The National Supervisory Authority for Personal Data Processing (ANSPDCP) has gradually evolved from a procedural enforcer to an ethical co-interpreter of EU values. Its decisions increasingly reference principles such as proportionality and dignity, and recent jurisprudence indicates a willingness to consider the broader social implications of sensitive data processing.[10] As such, Romania exemplifies what Hijmans describes as "polycentric governance" in EU data protection—a model in which national regulators act not as subordinates but as autonomous participants in a shared constitutional project.[11]

---

[3] Charter of Fundamental Rights of the European Union, OJ C 326/391, 26 October 2012, Article 1.

[4] Christopher Kuner, Lee A. Bygrave, and Christopher Docksey, eds., ***The GDPR: A Commentary*** (Oxford: Oxford University Press, 2020), 295–312.

[5] Paul Nemitz, "Constitutional Democracy and Technology in the Age of Artificial Intelligence," *Philosophical Transactions of the Royal Society A* 376, no. 2133 (2018): 20180089. DOI: 10.1098/rsta.2018.0089. Natea Mihaela Daciana, Fabricating truth: from a hybrid war to political fake news. Study case on Romanian illiberal parties' discourse in the context of the Ukrainian war, Civil Szemle, Special Issues V/2023, pp. 155-168

[6] Giovanni Sartor, "A Risk-Based Approach to Data Protection," *Philosophical Transactions of the Royal Society A* 380, no. 2238 (2022): 20210192. DOI: 10.1098/rsta.2021.0192.

[7] Alessandro Mantelero, "AI and Data Protection: Challenges and Possible Remedies," ***Computer Law & Security Review*** 37 (2020): 105–134. DOI: 10.1016/j.clsr.2020.105400.

[8] European Commission, ***Artificial Intelligence Act***, COM(2021) 206 final, 2024.

[9] European Commission, *Ethics Guidelines for Trustworthy Artificial Intelligence*, High-Level Expert Group on AI, 2019.

[10] ANSPDCP, *Annual Activity Report 2024* (Bucharest: ANSPDCP, 2024), https://www.dataprotection.ro.

[11] Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU* (Cham: Springer, 2016), 301–306.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

Nonetheless, the mere existence of ethical norms does not guarantee their internalisation within either public administration or private industry. There remains a gap between regulatory ambition and practical implementation, especially in sectors driven by rapid technological innovation. The OECD has noted that jurisdictions with robust data protection regimes tend to exhibit higher levels of digital trust and economic resilience, suggesting that ethical regulation may serve as a competitive asset rather than a constraint.[12] However, this depends on cultivating a culture of accountability, transparency, and risk anticipation—values that must be embedded into legal education, institutional practice, and technological design from the outset.

The legal architecture of Article 9 GDPR reflects a sophisticated balance between individual rights and collective interests, grounded in a deontological ethical tradition that defines the European regulatory approach. Unlike data protection laws in other jurisdictions, such as the United States, where privacy is often interpreted as a property or contractual right, the European conception views data protection as a matter of **human dignity and non-discrimination**. This distinction is pivotal: it informs not only the substantive content of the regulation but also the procedural mechanisms through which it is enforced. The enumeration of specific categories of sensitive data—race, religion, political opinion, health, and so on—mirrors the protected grounds in EU anti-discrimination law, particularly Articles 20 and 21 of the Charter of Fundamental Rights.[13] This alignment affirms that data protection serves not merely to avoid economic harm or reputational loss but to preserve the **moral and legal integrity of the person**.

The principle of proportionality, long established in European public law, serves as a mediating doctrine between competing rights and policy objectives.[14] When applied to data processing, it requires that any interference with sensitive data be **suitable**, **necessary**, and **proportionate in the strict sense** – i.e., that the benefits of processing outweigh the risks to individual rights and cannot be achieved by less intrusive means. This is not a formality but a substantive standard that obliges data controllers to engage in contextual risk assessment. Such evaluations are central to **data protection impact assessments (DPIAs)** mandated under Articles 35 and 36 GDPR, particularly where large-scale processing of sensitive data or the use of new technologies is involved.[15] In this sense, proportionality becomes both a **legal test** and an **ethical filter**, operationalising human dignity into decision-making processes.

This legal-philosophical framework gains even more complexity in light of the **emergent capabilities of artificial intelligence systems**, which are able to infer sensitive traits from data that is, on the surface, non-sensitive. Recent studies in computational social science demonstrate how machine learning algorithms can predict mental health conditions, sexual orientation, or political views based solely on metadata or behavioural patterns.[16] This raises profound concerns not only about privacy but about **informational autonomy** – the ability of individuals to control what others know about them. The collapse of the boundary between sensitive and non-sensitive data, as observed by Mantelero and others, compels regulators to adopt a more **contextual and dynamic understanding of sensitivity**.[17]

Indeed, Article 9 GDPR was not designed with these inferential capacities in mind. However, its moral logic remains highly applicable. The presumption of illegality that governs sensitive data

[12] OECD, *Digital Economy Outlook 2022* (Paris: OECD Publishing, 2022), 117–122. DOI: 10.1787/5b2e4f8a-en.
[13] Charter of Fundamental Rights of the European Union, Articles 20–21, OJ C 326/391, 2012.
[14] Armin von Bogdandy, "Proportionality in European Public Law," *Common Market Law Review* 47, no. 4 (2010): 1171–1210.
[15] European Data Protection Board, *Guidelines on Data Protection Impact Assessment*, WP248 rev.01, 2017.
[16] Sandra Wachter and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," *Columbia Business Law Review* 2022, no. 1 (2022): 494–620.
[17] Alessandro Mantelero, "Beyond Data Ownership: Reinventing Privacy, Data Protection and Data Sovereignty," *Computer Law & Security Review* 34, no. 2 (2018): 222–229.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

processing can be reinterpreted in the AI context as a **presumption of ethical caution**. Even if inferred data falls outside the strict categories of Article 9, the **risk-based approach** now advocated by European regulators encourages a functional, rather than formal, reading of sensitivity.[18] This approach has been partially codified in the AI Act, which mandates that high-risk AI systems undergo not only technical scrutiny but also ethical evaluations, including human oversight and transparency obligations.[19]

What emerges is a regulatory ecosystem where data protection, algorithmic governance, and fundamental rights intersect. Sensitive data, once seen as a fixed legal category, is now viewed as a relational construct—one that evolves depending on **technological affordances, social context, and regulatory interpretation**. This shift has significant implications for both compliance and innovation. It implies that ethical foresight must become a standard component of system design, especially in areas such as healthcare, education, employment, and public administration, where the stakes of incorrect or biased inferences are particularly high.

The adoption of the European Union's Artificial Intelligence Act in 2024 represents a pivotal step in the expansion of data protection principles into the algorithmic realm. Unlike earlier sectoral regulations, the AI Act adopts a **horizontal and risk-based approach**, classifying AI systems based on their potential to infringe upon fundamental rights. High-risk systems—defined to include those used in biometric identification, employment decisions, access to education, and health services—are subject to a comprehensive set of obligations, ranging from transparency to human oversight.[20] These obligations are not merely technical; they embody the ethical commitments already articulated in the GDPR, particularly through Article 9.

Crucially, the AI Act does not supersede the GDPR but complements it, creating a dual compliance structure in which both data governance and algorithmic governance intersect. Article 10 of the AI Act, which outlines data governance obligations for high-risk systems, requires that training, validation, and testing data be relevant, representative, and free of bias.[21] This indirectly reinforces the sensitivity logic of Article 9 GDPR by ensuring that data categories which may reveal protected attributes—such as health, race, or political opinions—are treated with elevated safeguards during system development and deployment.

This integration of ethical constraints into system design aligns with the normative vision laid out in the European Commission's ***Ethics Guidelines for Trustworthy AI***.[22] These guidelines explicitly link trustworthy AI to three core principles: **lawfulness, ethical soundness, and technical robustness**. Each of these principles can be mapped back to the GDPR's architecture, where lawfulness corresponds to Article 6 (legal basis), ethical soundness to Article 9 (sensitive data and moral boundaries), and robustness to Articles 25 and 32 (data protection by design and by default). The AI Act thereby extends the scope of data protection law from ex-post enforcement to ex-ante system configuration.

A further layer of coherence is visible in how both GDPR, and the AI Act embrace **human oversight** as a structural guarantee. Under Article 22 GDPR, individuals have the right not to be subject to a decision based solely on automated processing, including profiling, where such decisions produce legal or similarly significant effects.[23] The AI Act reinforces this by mandating that high-risk systems allow for meaningful human intervention, particularly where sensitive personal data is

[18] Giovanni Sartor, "A Risk-Based Approach to Data Protection," *Philosophical Transactions of the Royal Society A* 380, no. 2238 (2022): 20210192. DOI: 10.1098/rsta.2021.0192.
[19] European Commission, *Artificial Intelligence Act*, COM(2021) 206 final, Title III, Chapter 2, 2024.
[20] European Commission, *Artificial Intelligence Act*, COM(2021) 206 final, Title III, Chapter 1, Article 6, 2024.
[21] Ibid., Article 10.
[22] European Commission, *Ethics Guidelines for Trustworthy Artificial Intelligence*, High-Level Expert Group on AI, 2019.
[23] General Data Protection Regulation, Article 22, Regulation (EU) 2016/679.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

involved. This duality reflects the broader ambition of the EU to constitutionalise AI through mechanisms of accountability that go beyond transparency.

Romania, like other Member States, is required to transpose and apply the AI Act in ways that maintain consistency with existing data protection frameworks. The ANSPDCP, in collaboration with national digital authorities, will likely play a key role in monitoring high-risk AI deployments, especially in the public health and biometric surveillance sectors.[24] Given Romania's prior engagement with ethical data interpretation under Article 9 GDPR, its regulatory ecosystem is relatively well-positioned to absorb these obligations. However, this will require capacity-building, interdisciplinary training, and coordination between legal, technical, and ethical experts.

The interweaving of the AI Act and GDPR sets a precedent for how **future European digital legislation** may be structured. As the Commission advances initiatives like the European Health Data Space and the Digital Services Act, it becomes increasingly clear that the EU is constructing a layered legal order in which **fundamental rights are embedded as design principles**.[25] Sensitive data, once treated as a legal exception, is now becoming the ethical core around which entire regulatory regimes are being built.

Romania's domestic experience with the implementation of Article 9 GDPR offers a compelling case study in the Europeanisation of data protection norms and the progressive internalisation of ethical standards into national administrative practices. The Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), Romania's supervisory authority, has gradually evolved beyond its initial formalistic role to embrace a more **value-driven interpretation of sensitive data regulation**. This development is evident in several enforcement decisions and public reports which explicitly invoke the principles of **proportionality**, **necessity**, and **human dignity** as foundational to lawful data processing.[26] Such references echo the jurisprudential language used by the Court of Justice of the European Union (CJEU), creating normative coherence between Union-level and national-level reasoning.

One significant area of Romanian enforcement has been in the **healthcare sector**, particularly during the COVID-19 pandemic and in the subsequent deployment of digital health systems. In 2021 and 2022, the ANSPDCP issued multiple opinions on the legality of processing health-related data for purposes such as vaccination records, patient triage systems, and epidemiological tracking. In these cases, the authority emphasized that even where Article 9(2)(i) of the GDPR provides a legal basis for processing in the context of public health, controllers must still comply with **data minimisation** and **purpose limitation** principles under Articles 5(1)(c) and 5(1)(b).[27] These opinions show a willingness to **operationalise ethical constraints** into sectoral practices and to condition the use of sensitive data on substantive risk assessments.

Moreover, the Romanian authority has demonstrated **alignment with evolving EU doctrine** in its treatment of biometric and behavioural data. In its 2024 activity report, the ANSPDCP analysed the use of facial recognition technologies in public schools and retail environments, concluding that such systems pose elevated risks to informational autonomy and may fall within the high-risk category under the EU AI Act.[28] This proactive interpretation mirrors the European Data Protection Supervisor's (EDPS) growing concern about biometric surveillance and underscores Romania's commitment to anticipatory governance.

However, the Romanian context also reveals institutional and structural challenges that may hinder effective enforcement. The authority operates with **limited financial and human resources**,

[24] ANSPDCP, *Guidelines on the Application of Article 9 GDPR in Health Services* (Bucharest: ANSPDCP, 2025).
[25] European Commission, ***European Strategy for Data***, COM(2020) 66 final, Brussels, 2020.
[26] ANSPDCP, *Annual Activity Report 2023* (Bucharest: ANSPDCP, 2023), https://www.dataprotection.ro.
[27] General Data Protection Regulation, Articles 5(1)(b)–(c), Regulation (EU) 2016/679.
[28] ANSPDCP, *Annual Activity Report 2024* (Bucharest: ANSPDCP, 2024), p. 18.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

and the institutional independence required under Article 52 GDPR has occasionally been questioned in public debates.[29] Furthermore, coordination between ANSPDCP and other national bodies responsible for digital transformation, cybersecurity, and health informatics remains underdeveloped. This fragmentation undermines the holistic application of data ethics principles and suggests a need for integrated governance mechanisms capable of handling the **cross-sectoral complexity** of sensitive data regulation.

To address these issues, Romanian institutions must invest in **regulatory capacity-building**, including interdisciplinary training programs for staff, enhanced cooperation with civil society, and the adoption of internal ethical review protocols for AI and big data projects.[30] The implementation of such measures would not only improve compliance with EU law but also foster a **culture of ethical stewardship**—an essential condition for trustworthy innovation. By embedding fundamental rights into institutional routines and decision-making tools, Romania can strengthen its role within the **polycentric governance structure** of European data protection.[31]

The European Union's approach to the protection of sensitive personal data under Article 9 GDPR stands in stark contrast to the legal traditions of other major jurisdictions, most notably the United States. While the EU model is grounded in **human dignity and fundamental rights**, the American privacy landscape is characterized by a **sectoral and consumer-centric framework**, heavily reliant on contractual consent and tort-based remedies.[32] This divergence is not merely procedural but reflects **incompatible normative foundations**: whereas European law views data protection as an extension of personhood, U.S. law generally treats personal data as **property or commodity**, subject to market logics and private arrangements.

There is no federal equivalent in the United States to the GDPR or to Article 9's regime of heightened protection for sensitive data. Instead, privacy protections are scattered across industry-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Children's Online Privacy Protection Act (COPPA).[33] These laws are limited in scope and do not establish a unified rights-based framework. Importantly, none of these statutes contains a provision analogous to Article 9's **presumption of illegality** for processing sensitive data. As a result, American data controllers are not generally required to demonstrate necessity or proportionality in processing such information unless state law imposes stricter standards.

The absence of a **comprehensive federal privacy law** in the U.S. has led several states to enact their own regulations, such as the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA). These laws introduce some protections for sensitive data categories, including race, religion, and health, but they fall short of the **robust obligations and ethical constraints** imposed by the GDPR.[34] For example, while the CPRA requires businesses to provide opt-out options for the sale or sharing of sensitive data, it does not impose a **burden of justification** or mandate a DPIA for high-risk processing.

From a regulatory perspective, the EU model integrates **ex-ante safeguards** into system design, mandating data protection by default and by design (Articles 25–26 GDPR), while U.S. frameworks tend to emphasize **post-hoc accountability**, often through litigation or consumer

[29] European Union Agency for Fundamental Rights (FRA), *National Human Rights Institutions and Data Protection Authorities: Strengthening Synergies*, 2021.
[30] European Commission, *Better Regulation Guidelines*, SWD(2021) 305 final, Brussels, 2021.
[31] Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU* (Cham: Springer, 2016), 304–306.
[32] Paul Schwartz and Daniel Solove, "Reconciling Personal Information in the United States and European Union," *California Law Review* 102, no. 4 (2014): 877–916.
[33] Daniel J. Solove, "The Limits of Privacy," *Stanford Law Review* 94, no. 5 (2000): 1121–1168.
[34] California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

complaints.[35] Furthermore, the European emphasis on proportionality and necessity makes it possible to challenge data processing even in the absence of harm, whereas American law typically requires demonstrable injury to establish standing in court.[36] This difference has significant implications for **AI governance**, as systems trained on sensitive inferences may be lawful in the U.S. but illegal under EU law if they lack sufficient justification or oversight.

Notably, the **"Brussels Effect"**, as coined by Anu Bradford, has resulted in GDPR-inspired principles influencing non-European jurisdictions and multinational corporations.[37] Tech companies operating globally often adopt GDPR standards as a baseline for data handling practices, particularly when it comes to consent management, user transparency, and data minimisation. While this extraterritorial impact has partially raised standards worldwide, it has also highlighted the **normative gap** between the EU's rights-based approach and the **market-centric rationality** that continues to shape American privacy discourse.

These contrasts underline the originality and ambition of the EU's regulatory vision. By placing the **human person** at the centre of data governance, the GDPR and its interpretative culture challenge dominant techno-economic paradigms and assert a model of **ethical restraint over technical possibility**. As innovation accelerates in fields such as biometrics, neurotechnology, and predictive analytics, the divergence between these models may deepen, raising difficult questions about **interoperability, global standards, and cross-border enforcement**.

Building on the doctrinal and practical challenges outlined in the previous sections, it becomes essential to articulate a set of **concrete policy proposals** aimed at enhancing the enforceability and ethical robustness of Article 9 GDPR in both European and national contexts. These proposals respond to the increasing complexity of the data environment, the rise of AI-powered inference systems, and the pressing need to align innovation with fundamental rights.

First, it is necessary to **update the interpretative guidance of Article 9 GDPR** at the European level to explicitly account for **inferred sensitive data**. While the current text lists exhaustively the categories of sensitive personal data, it does not explicitly address the situation where non-sensitive inputs are used to predict sensitive attributes. Regulators should clarify through **European Data Protection Board (EDPB)** guidelines that inferred sensitive data falls within the scope of Article 9 when such inferences create significant risks of discrimination or identity exposure.[38] This clarification would help close an emerging gap between legal categories and technological realities.

Second, **risk-based enforcement** should be strengthened through a new generation of **sector-specific DPIA templates**, particularly in areas such as education, healthcare, public security, and insurance.[39] These templates should be co-developed by data protection authorities, industry bodies, and civil society, and incorporate ethical criteria such as distributive impact, power asymmetry, and group privacy concerns. A DPIA should not be a procedural checkbox but a tool for **ethical anticipation**, capable of detecting systemic harms before they materialise.

Third, **national data protection authorities** such as Romania's ANSPDCP should be institutionally reinforced through increased **budgetary allocations**, digital forensics capabilities, and legal staffing.[40] In addition, a **mandatory internal ethics officer** should be appointed in all public

[35] General Data Protection Regulation, Articles 25–26, Regulation (EU) 2016/679.
[36] Clapper v. Amnesty International USA, 568 U.S. 398 (2013).
[37] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020), 212–218.
[38] European Data Protection Board, *Guidelines 4/2022 on the Calculation of Administrative Fines under the GDPR*, EDPB, Brussels, 2022.
[39] European Data Protection Supervisor (EDPS), *Opinion on the Interplay between the AI Act and the GDPR*, Brussels, 2022.
[40] FRA, *Data Protection Authorities in the EU: Mapping Their Powers and Resources*, 2021.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

institutions and private entities processing sensitive data at scale. This officer would liaise with DPOs and ensure that ethical principles—such as dignity, necessity, and non-discrimination—are embedded into data governance routines.

Fourth, the **AI Act's implementation phase** must include robust **horizontal coordination** between supervisory authorities responsible for GDPR, AI, cybersecurity, and anti-discrimination. At the EU level, this could be realised through the establishment of a **Joint Ethics and Risk Assessment Board**, which would evaluate high-risk digital systems across multiple domains.[41] At the national level, Romania could pilot such inter-agency coordination by creating a **Digital Ethics Task Force** combining the ANSPDCP, the Digitalization Authority (ADR), and the Romanian National Council for Combating Discrimination (CNCD).

Fifth, **data literacy and civic education** programs should be embedded in school curricula and professional training schemes. These programs must go beyond basic digital hygiene and explain the **ethical significance of sensitive data**, the limits of consent in power-imbalanced settings, and the rights guaranteed by the GDPR.[42] A democratic data culture depends not only on laws and regulators but also on **informed and empowered individuals** capable of asserting their rights.

Finally, **academic institutions and research funders** must be encouraged to integrate GDPR and Article 9 considerations into **research ethics review protocols**, especially in medical, behavioural, and AI-driven studies. The European Commission should require all Horizon Europe projects dealing with personal data to include a dedicated **"sensitive data ethics appendix"** as part of their ethics assessment.[43]

Together, these proposals sketch a **multi-level governance model** for the future of sensitive data protection—one that combines legal authority, ethical foresight, institutional capacity, and public participation. Such a model would not only strengthen compliance with GDPR norms but also ensure that **data-driven societies remain anchored in shared values of dignity, fairness, and democratic accountability**.

In conclusion, the European Union's regulatory approach to the protection of sensitive personal data—anchored in Article 9 GDPR—represents not only a legal innovation but a profound **moral response to the challenges of the digital age**. By explicitly grounding data protection in the principles of **human dignity, equality, and proportionality**, the GDPR redefines the relationship between individual autonomy and technological power. Sensitive data are no longer treated as neutral or value-free informational elements; they are viewed as **symbolic extensions of personhood**, and their misuse constitutes a violation of fundamental rights rather than a mere breach of privacy.

The evolution of complementary legal instruments, including the **Artificial Intelligence Act**, confirms that the EU is consolidating a coherent model of **rights-based digital constitutionalism**. Within this model, data protection does not operate in isolation but interacts dynamically with principles of algorithmic transparency, ethical oversight, and systemic accountability. The **reversal of the burden of justification**—a core feature of Article 9—serves as a counterweight to the inherent asymmetries of power between data subjects and data controllers, especially in high-risk AI contexts.

Romania's implementation of Article 9, as evidenced by the growing sophistication of ANSPDCP enforcement and jurisprudential alignment with CJEU case law, illustrates how national actors can act as **ethical co-guardians** of Union values. Yet, enforcement alone is insufficient. As

[41] AlgorithmWatch, *Regulatory Cooperation in Europe: A Comparative Overview*, 2023.
[42] European Commission, *Digital Education Action Plan 2021–2027*, COM(2020) 624 final.
[43] European Commission, *Horizon Europe Ethics Appraisal Procedure Guidelines*, 2021, Natea Mihaela Daciana, The European Knowledge-Security Nexus: Science Diplomacy as a Policy Tool Against Hybrid Threats, Europolity-Continuity and Change in European Governance, nr6/2025

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3

the analysis has shown, legal norms must be **internalised through institutional routines, civic education, and interdisciplinary capacity**. Without a supportive ecosystem of governance, Article 9 risks remaining a symbolic provision rather than a practical shield.

The comparative perspective reveals that the EU model is not universally shared, particularly when contrasted with **market-centric regulatory frameworks** such as that of the United States. Nevertheless, the global diffusion of GDPR principles—the so-called **Brussels Effect**—indicates that Europe's normative leadership in data ethics is already shaping international standards.[44] This leadership is not based on coercion but on **moral coherence and regulatory sophistication**, which have made GDPR a reference point for trust in digital infrastructure.

Ultimately, the future of sensitive data protection will depend on our collective ability to **embed moral constraints into digital design**. As technologies become more invasive and capable of inferring intimate aspects of human identity, the ethical architecture of data protection must evolve accordingly. The GDPR, and Article 9 in particular, provide a valuable foundation for this evolution. But it is through sustained policy commitment, institutional learning, and cultural change that the European ambition to **civilise digital modernity** will be realised.[45] The lesson is not only legal—it is philosophical: that in a data-driven society, freedom requires law, and law requires ethics.

BIBLIOGRAPHY

AlgorithmWatch, *Regulatory Cooperation in Europe: A Comparative Overview*, 2023.
ANSPDCP, *Annual Activity Report 2023* (Bucharest: ANSPDCP, 2023), https://www.dataprotection.ro.
ANSPDCP, *Annual Activity Report 2024* (Bucharest: ANSPDCP, 2024), https://www.dataprotection.ro.
ANSPDCP, *Annual Activity Report 2024* (Bucharest: ANSPDCP, 2024), p. 18.
ANSPDCP, *Guidelines on the Application of Article 9 GDPR in Health Services* (Bucharest: ANSPDCP, 2025).
Bogdandy, Armin von, "Proportionality in European Public Law," *Common Market Law Review* 47, no. 4 (2010): 1171–1210.
Bradford, Anu, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020), 212–218.
California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq.
Charter of Fundamental Rights of the European Union, Articles 20–21, OJ C 326/391, 2012.
Charter of Fundamental Rights of the European Union, OJ C 326/391, 26 October 2012, Article 1.
Clapper v. Amnesty International USA, 568 U.S. 398 (2013).
Costea, Maria, Costea Simion, "Ukraine between EU and Eurasian Regional Project in 2013", p.113-131, in *Transylvanian Review*, Vol. XXIV, Supplement No. 1, 2015 DOI: 10.5281/zenodo.15564422
Daniel J. Solove, "The Limits of Privacy," *Stanford Law Review* 94, no. 5 (2000): 1121–1168.
European Commission, *Artificial Intelligence Act*, COM(2021) 206 final, 2024.
European Commission, *Artificial Intelligence Act*, COM(2021) 206 final, Title III, Chapter 2, 2024.
European Commission, *Artificial Intelligence Act*, COM(2021) 206 final, Title III, Chapter 1, Article 6, 2024.
European Commission, *Artificial Intelligence Act*, COM(2021) 206 final, Title III, Chapter 1, Article 10, 2024
European Commission, *Better Regulation Guidelines*, SWD(2021) 305 final, Brussels, 2021.
European Commission, *Digital Education Action Plan 2021–2027*, COM(2020) 624 final.
European Commission, *Ethics Guidelines for Trustworthy Artificial Intelligence*, High-Level Expert Group on AI, 2019. ("IRIS Merlin – Council of Europe")
European Commission, *European Strategy for Data*, COM(2020) 66 final, Brussels, 2020.
European Commission, *Horizon Europe Ethics Appraisal Procedure Guidelines*, 2021.

[44] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford: Oxford University Press, 2020), 215.
[45] Alain Supiot, *Homo Juridicus: On the Anthropological Function of the Law* (London: Verso, 2007), 149–150.

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-001-6

European Data Protection Board, *Guidelines 4/2022 on the Calculation of Administrative Fines under the GDPR*, EDPB, Brussels, 2022.
European Data Protection Board, *Guidelines on Data Protection Impact Assessment*, WP248 rev.01, 2017.
European Data Protection Supervisor (EDPS), *Opinion on the Interplay between the AI Act and the GDPR*, Brussels, 2022.
European Parliament and Council, *Regulation (EU) 2016/679 (General Data Protection Regulation)*, Article 9, OJ L119/1, 4 May 2016.
European Union Agency for Fundamental Rights (FRA), *National Human Rights Institutions and Data Protection Authorities: Strengthening Synergies*, 2021.
FRA, *Data Protection Authorities in the EU: Mapping Their Powers and Resources*, 2021.
General Data Protection Regulation, Article 22, Regulation (EU) 2016/679.
General Data Protection Regulation, Articles 25–26, Regulation (EU) 2016/679.
General Data Protection Regulation, Articles 5(1)(b)–(c), Regulation (EU) 2016/679.
Giovanni Sartor, "A Risk-Based Approach to Data Protection," *Philosophical Transactions of the Royal Society A* 380, no. 2238 (2022): 20210192. DOI: 10.1098/rsta.2021.0192.
Giovanni Sartor, "A Risk-Based Approach to Data Protection," *Philosophical Transactions of the Royal Society A* 380, no. 2238 (2022): 20210192. DOI: 10.1098/rsta.2021.0192.
Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU* (Cham: Springer, 2016), 301–306.
Kuner, Christopher; Lee A. Bygrave, and Christopher Docksey, eds., *The GDPR: A Commentary* (Oxford: Oxford University Press, 2020), 295–312.
Mantelero, Alessandro, "AI and Data Protection: Challenges and Possible Remedies," *Computer Law & Security Review* 37 (2020): 105–134. DOI: 10.1016/j.clsr.2020.105400.
Mantelero, Alessandro, "Beyond Data Ownership: Reinventing Privacy, Data Protection and Data Sovereignty," *Computer Law & Security Review* 34, no. 2 (2018): 222–229.
Natea, Mihaela Daciana; Costea, Maria; Costea, Simion. *EU Security and Multicultural Societies. Dealing with a Russian Empire Revival*, Paris, L'Harmattan, 2024
Natea, Mihaela Daciana; Costea, Simion (eds), *EU Law and Politics at the Crossroads: Navigating the Complexities of AI, Digitalization, Data Protection, Security, and Radicalization (L'Europe unie/United Europe, Paris, 20/2023, special volume),* Cluj-Napoca: Napoca Star, 2023. DOI 10.5281/zenodo.15182658
Natea Mihaela Daciana, Fabricating truth: from a hybrid war to political fake news. Study case on Romanian illiberal parties' discourse in the context of the Ukrainian war, Civil Szemle, Special Issues V/2023, pp. 155-168
Natea Mihaela Daciana, The European Knowledge-Security Nexus: Science Diplomacy as a Policy Tool Against Hybrid Threats, Europolity-Continuity and Change in European Governance, nr6/2025
Natea, Mihaela Daciana; Costea, Simion (eds), *The EU foreign and security dilemmas in a challenging world (L'Europe unie/United Europe 19/2023, special volume)* Cluj- Napoca: Napoca Star, 2023
Nemitz, Paul, "Constitutional Democracy and Technology in the Age of Artificial Intelligence," *Philosophical Transactions of the Royal Society A* 376, no. 2133 (2018): 20180089. ("Full article: Democratization in the age of artificial intelligence ...") DOI: 10.1098/rsta.2018.0089.
OECD, *Digital Economy Outlook 2022* (Paris: OECD Publishing, 2022), 117–122. DOI: 10.1787/5b2e4f8a-en.
Schwartz, Paul and Daniel Solove, "Reconciling Personal Information in the United States and European Union," *California Law Review* 102, no. 4 (2014): 877–916.
Supiot, Alain, *Homo Juridicus: On the Anthropological Function of the Law* (London: Verso, 2007), 149–150.
Wachter Sandra, and Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI," *Columbia Business Law Review* 2022, no. 1 (2022): 494–620. ("Paper: A Right to Reasonable Inferences: Re-Thinking Data Protection ...")

Print ISSN 0248-2851 • On-line/Linking ISSN 2743-4052 • ISBN 978-630-354-213-3