European Journal of Law and Public Administration
ISSN: 2360-6754 | e-ISSN: 2559-7671
Covered in: Erih Plus; HeinOnline; CEEOL; RePEc; CrossRef; Google Scholar; KVK; WorldCat; ICI Journals Master List - Index Copernicus; EBSCO.

2025, Volume 12, Issue 1, pages: 89-97 | https://doi.org/10.18662/eljpa/12.1/258

Black Box AI and the Sovereignty of Personal Data: Between GDPR and Digital Ethics

Andreea BURUIANĂ (m. RUSU) [1]

[1] PhD candidate at "Titu Maiorescu" Doctoral School of Law of Bucharest, Romania; https://orcid.org/0009-0000-1535-7270

Abstract: *The emergence of Black Box artificial intelligence poses fundamental challenges to data protection law, particularly with regard to digital sovereignty and the application of the General Data Protection Regulation (GDPR). These algorithmic systems, defined by their lack of transparency and the inability to explain automated decisions, significantly hinder the exercise of guaranteed rights such as data access, objection, and the right to contest automated decisions. Although the GDPR enshrines the principle of transparency and imposes clear obligations on data controllers, opaque AI systems jeopardize the informational autonomy of individuals. The CJEU ruling in the Nowak case reinforces the right to understand the decision-making logic of AI, but practical implementation remains difficult due to trade secret protections. In this context, an expanded legal framework is necessary—one that integrates explainability requirements and ethical accountability to ensure a balance between innovation and the protection of fundamental rights. Furthermore, the distinction between formal transparency and substantive explainability becomes critical in guaranteeing individuals' effective control over the data and decisions that affect them.*

Keywords: *Black Box; GDPR; AI; protection; personal data; digital ethics.*

How to cite: Buruiană, A. (2025). Black box AI and the sovereignty of personal data: between GDPR and digital ethics. *European Journal of Law and Public Administration, 12*(1), 89-97. https://doi.org/10.18662/eljpa/12.1/258

©2025 Published by In Manifest Network in partnership with LUMEN Publishing. This is an open access article under the CC BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

Introduction

A new and increasingly pressing challenge in the legal field of personal data protection is represented by the rise of *Black Box* artificial intelligence, which has generated significant concerns among legal scholars and academics regarding personal data sovereignty and the implications of applying the General Data Protection Regulation (GDPR) to digital ethics and individual fundamental rights. The term "*Black Box AI*" refers to those artificial intelligence systems whose decision-making logic is opaque and difficult to interpret by humans, thus raising important issues of accountability, transparency, and ethical governance (Chaudhary, 2024). As these algorithmic systems become increasingly embedded in daily life, tensions between individual rights and technological capabilities are intensifying, bringing critical questions about data control and privacy to the forefront.

Black Box AI technologies are primarily distinguished by decision-making opacity. The algorithms used fail to provide intelligible justifications for how data are processed and results produced. This lack of transparency becomes problematic when such systems process personal data, undermining the informational autonomy and digital sovereignty of individuals. Within the European Union, the GDPR remains the only binding normative framework governing this area. However, the emergence of autonomous AI introduces new legal challenges, particularly concerning the rights guaranteed under Articles 8 and 21 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention on Human Rights.

Data sovereignty refers to the individual's right to exercise control over their own data and its use. In a digital context where AI systems increasingly function as black boxes, the challenge of guaranteeing this control becomes essential. Many users are unaware of how their data are collected and used, which may result in violations of the right to privacy (Mbah, 2024). The ethical implications of these practices are profound, as individuals may become victims of algorithmic discrimination or cognitive manipulation, without their informed consent or awareness (Hoxhaj et al., 2023).

Regulatory frameworks, such as the GDPR, aim to address these concerns by establishing clear standards for personal data processing. The GDPR imposes obligations related to transparency, and guarantees rights such as access, rectification, and erasure. However, the effective implementation of these principles is hindered in the case of Black Box AI, due to the unintelligibility of algorithmic logic, which may compromise the

full exercise of rights guaranteed by the Regulation. Additionally, the interaction between GDPR and digital sovereignty must be analyzed to understand its impact on ethical governance. Cross-border data flows and the presence of global economic actors have significantly complicated legal oversight, generating tensions between national regulations and global technological practices. The obligation of algorithmic transparency—a key pillar of digital ethics—must be reconciled with the competitive pressures faced by companies operating advanced AI systems.

The Principle of Transparency and the Limits of Opaque Artificial Intelligence

The rapid advancement of artificial intelligence technologies has generated growing concern over the transparency of algorithmic processes, especially in systems based on Black Box AI, where the decision-making mechanisms remain opaque. This challenge is particularly salient in the context of the General Data Protection Regulation, which emphasizes the rights of data subjects and imposes specific requirements regarding transparency and explainability (Huang, 2025). As organizations increasingly integrate these technologies, a careful balance must be achieved between AI benefits and the protection of fundamental rights.

At the heart of the GDPR lies a commitment to transparency, which obligates data controllers to inform individuals about the processing of their personal data (Tzimas, 2023). Article 5(1)(a) of the GDPR enshrines the principles of lawfulness, fairness, and transparency in data processing. The fundamental issue lies in the difficulty of translating algorithmic outputs into intelligible and accessible information for data subjects. This limitation not only complicates compliance but also risks violating individuals' rights to be informed and to understand how their data are used (Chaudhary, 2024).

The concept of algorithmic transparency is further complicated by the explainability requirements under the GDPR. To fulfill the obligations under Articles 13 and 14, data controllers must provide clear and comprehensible explanations for automated decision-making processes (Nisevic et al., 2024). However, many AI systems, particularly those based on machine learning, operate in ways that defy simple explanations, making legal compliance increasingly difficult. This is especially relevant given the right to contest automated decisions, as guaranteed by the GDPR, which not only implies access to an explanation, but also a real understanding of the underlying decision-making mechanisms and the ability to challenge them effectively.

To operationalize algorithmic transparency, it is essential to consider the implications of the Court of Justice of the European Union's (CJEU) ruling in the *Nowak*(Case C-434/16) case. The CJEU affirmed the right of individuals to obtain meaningful information about the logic involved in automated decisions that affect them (Papadimitriou, 2023). This landmark decision raises significant operational challenges for organizations using Black Box AI systems, as the required level of transparency may conflict with trade secrets and technological know-how. This reinforces the need for a more rigorous transparency framework, aligned with GDPR provisions. The judgment also affirms that algorithmic opacity can undermine individuals' fundamental rights, limiting their capacity to effectively contest AI-based decisions. Consequently, AI developers must navigate a complex landscape, where legal obligations and technical limitations intersect—sometimes at the expense of innovation (Nisevic et al., 2024).

The interconnection between transparency and accountability has recently been emphasized in the academic literature, which advocates for stricter regulatory measures aimed at the ethical distribution of AI technologies (Nnawuchi et al., 2024). Critical analyses show that the current legal framework is insufficient to address the complexity of algorithmic transparency, requiring dynamic legislative adaptations. However, merely establishing legal requirements does not guarantee actual transparency. An ethical dimension must also be integrated, especially regarding the subtle influence of algorithmic distortions on fundamental rights. As the discourse on AI governance evolves, it becomes essential to strike a balance between data protection and innovation, emphasizing the distinction between formal transparency and substantive explainability, and promoting mechanisms that contextualize and translate algorithmic decisions into meaningful content for the individuals affected (Vorras & Mitrou, 2021).

Digital Sovereignty and the Right to Privacy in ECtHR Jurisprudence

An analysis of the jurisprudence of the European Court of Human Rights (ECtHR) reveals its essential role in resolving disputes at the intersection of digital sovereignty and the right to privacy. The Court's case law aims to establish a balance between state interests in digital sovereignty—such as national security and public order—and the individual's fundamental rights, particularly the right to respect for private life, as enshrined in Article 8 of the European Convention on Human Rights, with direct reference to the right to the protection of personal data.

A landmark case illustrating this balance is *S. and Marper v. the United Kingdom(Application nos. 30562/04 and 30566/04)*, where the ECtHR

examined the retention of DNA samples and fingerprints from individuals who had been acquitted. The Court found that the indiscriminate retention of such personal data constituted a violation of the right to private life under Article 8. The decision emphasized the need to strike a delicate balance between the state's interest in crime prevention and the individual's right to privacy. This principle was reaffirmed in *Big Brother Watch v. the United Kingdom*(*Applications nos. 58170/13, 62322/14 and 24960/15)*, where the Court assessed the legality of mass communications surveillance and underscored the need for strict legal safeguards to protect privacy in the context of state monitoring (Lubin, 2022).

These rulings make clear the inherent tension between the concept of digital sovereignty and the right to private life. States may invoke their sovereign right to regulate and oversee digital spaces, arguing such measures are necessary for public order and national security. While the ECtHR recognizes legitimate state interests, it insists on the existence of robust oversight mechanisms designed to prevent abuses. This tension also emerges in the broader context of privacy rights when data is collected and processed by public authorities (Yilma, 2023). States thus assume a dual role—as both protectors and potential violators of human rights. Although the state has a duty to protect its citizens, this obligation must not infringe upon fundamental rights, especially in an increasingly digitalized world. ECtHR decisions reflect this tension, generally positioning the state's protective role in relation to the risks posed by intrusions into private life.

The challenge of reconciling digital sovereignty with the right to privacy is exacerbated by rapid technological progress. Digitalization presents novel challenges to traditional human rights protection structures, necessitating adaptive legal interpretations and innovative safeguards to avoid neglect. Legal efforts to introduce protections against intrusive data collection practices are essential, especially in light of the risks associated with obtaining digital evidence in the context of human rights (Schmahl, S., 2022).

The intrusion into private life through surveillance extends beyond individual rights and touches on fundamental social values, including democracy itself. For instance, while facial recognition technologies may enhance public safety, they also raise serious concerns regarding civil liberties and human rights. Through rulings such as *S. and Marper* and *Big Brother Watch*, the ECtHR reaffirms its commitment to maintaining a balance between digital sovereignty and the right to private life. Although states retain the right to assert sovereignty in the digital space, there are critical limits that must be respected to safeguard fundamental rights. As surveillance practices evolve, legal interpretations and protective guarantees

must adapt to ensure that privacy is not sacrificed in an increasingly interconnected society. Through its jurisprudential developments, the ECtHR remains a vital bulwark against the potential erosion of privacy in the face of growing state interests.

The Need for an Expanded Ethical-Legal Framework

The rapid development and implementation of artificial intelligence (AI) systems have generated significant ethical and legal challenges, leading to the urgent need to integrate ethical principles into regulatory frameworks—particularly in the context of the European Union's Artificial Intelligence Act (AI Act). The importance of embedding these ethical principles lies in their capacity to uphold fundamental rights, safeguard privacy, and ensure individual autonomy.

Fundamental rights are at the core of democratic societies, and the introduction of AI-based technologies can threaten these rights if left unregulated. AI systems, even unintentionally, may infringe upon human rights, leading to discrimination and inequality. The AI Act seeks to address such concerns by establishing a regulatory framework that emphasizes fairness and non-discrimination in algorithmic decision-making processes. Integrating ethical principles such as transparency and accountability is essential to ensure that AI systems operate in a manner consistent with the respect for fundamental rights.

AI systems' ability to collect, store, and analyze vast amounts of personal data raises serious concerns regarding data protection and privacy. Transparent data management procedures and a strong ethical commitment to data use are indispensable for maintaining public trust in AI. The AI Act's provisions on data transparency underscore the importance of ethical standards in protecting private life. When ethical guidelines are aligned with legal obligations, the right to privacy can be defended more effectively against potential misuse of AI systems (Kharitonova, Y.S., 2023).

Individual autonomy is also impacted by the expansion of AI technologies. The capacity of such systems to influence decision-making—from personalized advertising to automated recruitment processes—raises critical questions about individuals' ability to maintain control over their choices. The ethical dimension of AI use requires legal structures that preserve the status of individuals as autonomous agents, free from undue manipulation. The AI Act proposal recognizes this imperative by promoting user-empowerment mechanisms, thereby reinforcing the ethical necessity of respecting human agency in the face of technological progress (Bosoer et al., 2023).

Simultaneously, algorithmic bias remains a pressing concern requiring a robust ethical-legal structure. Biased AI systems can perpetuate existing inequalities, undermining efforts to ensure fair treatment across various sectors. The AI Act seeks to mitigate these risks by introducing rules that promote non-discrimination and fairness in AI applications. By embedding ethical considerations within the legal framework, legislators can help prevent the exacerbation of social inequalities and support social justice.

Ultimately, the integration of ethical principles into AI legislation is not merely a regulatory formality; it represents a fundamental shift in how society interacts with intelligent technologies. Collaboration between ethicists, researchers, and legal scholars is essential to develop a normative framework capable of addressing moral dilemmas without stifling innovation. As AI technologies continue to evolve, prioritizing ethical principles within legal structures is indispensable for protecting fundamental rights, ensuring privacy, and upholding individual autonomy—values that are foundational to any democratic society in the face of emerging technological challenges.

Conclusions

The study has shown that as artificial intelligence (AI) systems continue to evolve, ensuring ethical compliance and transparency in automated decision-making processes becomes essential. This concern has sparked growing interest in mechanisms such as ethical regulatory sandboxes, which allow for technological innovations to be tested under regulatory supervision while respecting fundamental rights. Such frameworks help to build trust in digital ecosystems while acknowledging the dynamic and potentially disruptive nature of AI technologies.

Algorithmic transparency plays a key role in reducing the tensions discussed. By enhancing the explainability of automated decisions, stakeholders can better understand how data is processed and how decisions are made. In this way, individuals are empowered—both legally and ethically—to make informed decisions about their data. Furthermore, the development of trustworthy AI systems that comply with GDPR standards is crucial to effectively realizing data sovereignty in practice.

The interaction between opaque AI, personal data sovereignty, and GDPR standards highlights the urgent need for a robust framework of digital ethics. The regulatory environment must evolve to reflect the complexity of data governance in the AI era. Ensuring the respect of individual rights and fostering a predictable normative climate are vital conditions for shaping a fair, responsible, and transparent digital future.

Ensuring algorithmic transparency in Black Box systems under the GDPR presents significant challenges, particularly in relation to the rights of data subjects. The Court of Justice of the European Union's (CJEU) ruling in the Nowak case emphasized the need for AI systems to operate within a normative framework that promotes both explainability and transparency. In the future, collaboration between policymakers and technology experts will be critical in developing comprehensive regulations that balance technological complexity with the protection of fundamental rights, thereby securing a fair equilibrium between innovation and accountability. Such a collaborative approach could decisively shape the future of AI governance, aligning with the mandates of the GDPR and evolving societal expectations.

In conclusion, the intersection of opaque AI, personal data sovereignty, and GDPR regulations underscores the pressing need to develop a resilient and ethical digital framework. Regulatory systems must adapt to the increasing complexity of data governance in the age of AI. Respecting individual rights and strengthening a predictable legal framework are essential steps toward shaping a fair, responsible, and transparent digital society.

References

Bosoer, L., Cantero Gamito, M., & Rubio-Marin, R. (2023). Non-discrimination and the ai act. *Law and Digitalization. Arazandi.*

Chaudhary, G. (2024). Unveiling the black box: Bringing algorithmic transparency to AI. *Masaryk University Journal of Law and Technology, 18*(1), 93-122.

Hoxhaj, O., Halilaj, B., & Harizi, A. (2023). Ethical implications and human rights violations in the age of artificial intelligence. *Balkan Social Science Review, 22*(22), 153-171. https://doi.org/10.46763/BSSR232222153h

Huang, H. (2025). *Hiding in plain sight: Algorithmic transparency and explainability under the GDPR: Legal and technical challenges in applying the GDPR's provisions on transparency and explainability to algorithmic AI systems.* [Master's Thesis in European Union Law 30 ECTS] pp.22-23.https://uu.diva-portal.org/smash/get/diva2:1941957/FULLTEXT01.pdf

Kharitonova, Y. S. (2023). Legal means of providing the principle of transparency of the Artificial Intelligence. *Journal of Digital Technologies and Law, 1*(2).

Lubin, A. (2022). Big Brother Watch v. UK (Eur. Ct. HR Grand Chamber*). International Legal Materials, 61*(4), 605-653. https://doi.org/10.1017/ilm.2022.2

Mbah, G. O. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. *International Journal of Science and Research Archive, 13*(2). https://www.researchgate.net/profile/Geraldine-

Mbah/publication/387025413_Data_privacy_in_the_era_of_AI_Navigating_regulatory_landscapes_for_global_businesses/links/675c9d8cebc8f979702cae20/Data-privacy-in-the-era-of-AI-Navigating-regulatory-landscapes-for-global-businesses.pdf

Nisevic, M., Cuypers, A., & De Bruyne, J. (2024, June). Explainable AI: Can the AI Act and the GDPR go out for a date?. *In 2024 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE. https://doi.org/10.1109/IJCNN60899.2024.10649994

Nnawuchi, U., George, C., & Kammueller, F. (2024, September). Transparency vs explanation of machine learning algorithms: perspectives from recent legal proceedings. In *EPIA Conference on Artificial Intelligence* (pp. 270-283). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-73497-7_22

Papadimitriou, E. (2023). The right to explanation on the processing of personal data with the use of AI systems. *International Journal of Law and Changing World, 2*, 43. https://doi.org/10.54934/ijlcw.v2i2.53

Schmahl, S. (2022, September). Digitalisation and International Human Rights Law: Opportunities and Critical Challenges. In Digital *Transformations in Public International Law* (pp. 135-178). Nomos Verlagsgesellschaft mbH & Co. KG. https://www.nomos-elibrary.de/10.5771/9783748931638-135.pdf

Tzimas, T. (2023). Algorithmic transparency and explainability under EU law. *European Public Law, 29*(4). https://doi.org/10.54648/euro2023021

Vorras, A., & Mitrou, L. (2021). Unboxing the black box of artificial intelligence: algorithmic transparency and/or a right to functional explainability. In *EU Internet Law in the Digital Single Market* (pp. 247-264). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69583-5_10

Yilma, K., (2023). *Privacy and the role of international law in the digital age*. Oxford University Press