Artificial Intelligence and the Right to Privacy: Examination of the Legal Challenges Facing the Deployment of Artificial Intelligence in the Age of Automated Decision-Making

Ebenezer Amadi
Independent researcher & legal practitioner

ABSTRACT

Artificial intelligence (AI) systems deployed in the processing of data increasingly influence decision making in various sectors including healthcare, employment, finance, hospitality, and public governance. While these technologies enhance service delivery and provide efficient and predictive analysis, they also raise serious concerns regarding the protection of privacy and fundamental human rights. The research examines the implications of AI-driven automated decision-making on the right to privacy, with focus on the legal challenges facing the deployment of AI in automated decision-making. The research problem is whether the existing legal frameworks adequately safeguard fundamental rights of individuals against privacy risks arising from algorithmic systems, profiling activities, and reduced human oversight. The objective of this research is to critically assess the extent to which the existing legal regimes, particularly the EU's General Data Protection Regulation (GDPR) and EU Artificial Intelligence Act address the privacy concerns arising from deployment of AI technologies. I adopted the Doctrinal methodology involving a systematic analysis of primary and secondary sources of law which include statutes, subsidiary instruments, case laws, scholarly literature on data protection and AI governance. This study finds that while the GDPR introduced foundational principle such as the right not to be subject to solely automated decisions, data minimization, accountability and transparency obligations, the EU AI Act introduced a complementary risk-based approach, enacting strict requirements for high-risk AI technologies, improved accountability, and oversight mechanisms. However, significant gaps remain, especially concerning algorithmic opacity, limited practical enforceability of transparency rights, and insufficient guarantees of meaningful human intervention. These challenges undermine individual autonomy and privacy. This study is significant in advancing scholarly and policy debates on AI regulation and privacy protection by identifying structural weaknesses in existing legal frameworks. It concludes that more robust and harmonized regulatory measures are necessary. This research recommends strengthening transparency standards, improving accountability for AI developers and deployers, and ensuring effective human oversight to protect privacy and human rights in the digital era.

KEYWORDS
Artificial intelligence, Legal, Privacy, Policy

I. INTRODUCTION

Artificial intelligence technologies have advanced the decision-making process across sectors such as finance, health, marketing and public governance. AI systems are used to analyze large datasets, identifying behavioural patterns of individuals, and generate predictive behaviours that influence vital social and economic outcomes. Both the private

and public sectors increasingly depend on algorithmic systems for various results such as employment screening, credit scoring, predictive policing, and healthcare diagnostics.
Despite the significant benefits created by these AI technologies, the rapid use of AI systems raises serious concerns regarding the protection of privacy and fundamental rights of individuals. AI systems depend extensively on large datasets that often include personal information such as behavioural data, biometric data, and digital activity records. The collection and analysis of such data may lead to intrusive surveillance practices and extensive profiling of individuals.

Privacy is acknowledged as a fundamental right in democratic societies. However, deployment of AI challenges traditional legal approaches to privacy protection. Traditional data protection frameworks were particularly designed for identifiable and transparent data processing environments, whereas AI technologies often function through complex algorithmic models that are difficult to interpret.

The automated algorithmic decision-making also raises concern regarding compliance with the principles of data protection such as fairness, transparency, accountability and lawfulness. Individuals are subjected to algorithmic decisions that significantly affect their rights and opportunities without understanding how those decisions were made. Scholars described this problem as "black-box problem," referring to the opacity of algorithmic decision-making processes.

These issues surrounding the deployment of AI technologies prompted regulatory efforts focused on addressing the various legal challenges caused by AI systems. The EU's GDPR introduced safeguards designed to protect individuals from risk associated with automated decision-making. However, the EU GDPR made provisions for the tradition data protection standards which did not properly address the development of AI technologies. The rapid development of AI technologies continues to challenge the effectiveness of existing regulatory frameworks.

In response to the challenges facing the use of AI technologies, legal frameworks such as the GDPR and, more recently, the EU Artificial Intelligence Act were introduced to establish safeguards aimed at protecting fundamental rights. While these frameworks represent important steps forward, their effectiveness remains subject to debate.

This article critically examines the extent to which these regulatory frameworks adequately address the privacy risks associated with AI-driven automated decision-making. It argues that although they provide important protections, significant gaps remain, necessitating further regulatory innovation to safeguard privacy and human rights of people.

II. CONCEPTUAL AND THEORETICAL FRAMEWORK

The concept of privacy has undergone significant evolution over time. Early formulations, such as those advanced by Warren and Brandeis, conceptualized privacy as the "right to be let alone." However, as technological developments transformed the nature of information processing, legal understandings of privacy expanded to encompass informational control.In contemporary legal discourse, privacy is increasingly understood through the lens of informational self-determination, a principle that affirms an individual's authority over the collection, processing, and disclosure of personal data. This conception

has had a profound impact on European legal regimes, where privacy is entrenched as a fundamental right, notably under Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

Judicial interpretations have further shaped the scope of this right. In Katz v United States, the United States Supreme Court developed the 'reasonable expectation of privacy' standard, thereby moving away from a strictly property-based conception of privacy toward one centred on the individual's expectations. In a similar vein, the House of Lords in Campbell v MGN Ltd affirmed that the right to privacy encompasses protection against the misuse of private information. In the case, the court held that the appropriate test is whether a reasonable person of ordinary sensibilities, placed in the claimant's position, would regard the disclosure as offensive. On the facts, the claimant's therapy details were considered inherently private, giving rise to an enforceable obligation of confidentiality.

These developments reflect an increasingly better understanding of privacy as a dynamic and context-dependent right. However, the speedy rise of AI presents new challenges that strain these traditional frameworks of privacy and data protection.

AI technologies function within a data-driven ecosystem, where the collection and analysis of personal data are central to the result, they produce. AI system cannot operate without the collection of data. In this environment, privacy risks are no longer limited to discrete acts of intrusion but arise from continuous and often invisible data processing activities.

A defining feature of artificial intelligence systems is their dependence on the aggregation of vast quantities of data, allowing for the detection of patterns and relationships that would ordinarily escape conventional methods of analysis. Although this capacity significantly improves predictive performance, it simultaneously gives rise to concerns regarding disproportionate data collection and the attendant risk of improper use.

Furthermore, AI systems often engage in profiling, defined under the GDPR as any form of automated processing used to evaluate personal aspects relating to an individual. AI has the capacity to automatically profile individuals through the machine learning and algorithm. Profiling can lead to decisions that significantly affect individuals, including the denial of credit, employment opportunities, or access to services. The cumulative effect of these practices is a shift from reactive privacy protection focused on preventing specific harms to a more complex landscape where risks are systemic and difficult to detect.

Artificial intelligence systems are characteristically built upon the large-scale collection and integration of data, enabling them to uncover patterns and correlations that are often beyond the reach of traditional analytical techniques. While this capability enhances their predictive efficiency, it also raises important concerns about overbroad data harvesting and the heightened risk of misuse. AI technologies, particularly those used in targeted marketing, advertising and behavioural prediction, have the capacity to influence individuals' decisions in subtle but significant ways. This raises questions about manipulation and consent, as individuals may not fully understand how their data is being used to shape their behaviour.

Scholars have argued that this form of "informational asymmetry" undermines the conditions necessary for meaningful autonomy. In this context, the protection of privacy becomes vital not only for protecting personal data but also for preserving democratic values.

III. PRIVACY RISKS IN AUTOMATED DECISION-MAKING

Automated Decision-Making (ADM) poses extensive privacy risks, caused by the potential of AI to analyse, aggregate, and infer behaviour from large datasets, usually without any human oversight. These AI systems create critical challenges for data protection principles. The key privacy risks in Automated Decision-Making (ADM) include:

A. Data Aggregation and Surveillance

One of the most significant risks associated with AI is the potential for large-scale surveillance. AI system has the capacity to collect and analyse vast amounts of data and this enables both state and private actors to monitor individuals' behaviour in unprecedented ways.

The judgment of the Court of Justice of the European Union in Digital Rights Ireland Ltd v Minister for Communications underscores the legal boundaries of such practices. The Court concluded that the blanket retention of telecommunications data amounted to a disproportionate interference with the right to privacy. This case highlights the tension between technological capabilities and fundamental rights, emphasizing the need for strict safeguards in data processing.

B. Profiling and Discrimination

AI technologies have the potential to profile individuals. The AI-driven profiling raises serious concerns about discrimination and fairness. Machine learning models are trained on historical data, which may reflect existing social biases. As a result, these systems can perpetuate or even amplify discriminatory outcomes.

The case of State v Loomis provides a notable example. In that case, the use of a proprietary risk assessment algorithm in criminal sentencing raised concerns about transparency and bias. Although the court upheld the use of the tool, it acknowledged the limitations associated with its opacity.

Similarly, in the context of credit scoring, automated systems may disadvantage certain groups based on factors that correlate with protected characteristics, even if those characteristics are not explicitly considered.

C. Re-identification of Anonymized Data and Data Misuse

Another significant risk arises from the potential for re-identifying individuals from anonymized datasets. Advances in data analytics have demonstrated that combining datasets can reveal identities even where direct identifiers have been removed. This undermines one of the major assumptions underlying data protection law that anonymization effectively eliminates privacy risks.

D. Lack of Transparency and Accountability

Lack of Transparency and Accountability are one of the most fundamental risks posed by AI systems. Individuals are often unaware that their data is being processed or that algorithmic systems are influencing decisions that affect them. This lack of awareness

undermines the ability to exercise legal rights, including the right to access information and the right to challenge decisions.

The decision in R (Bridges) v Chief Constable of South Wales Police highlights the centrality of transparency as a condition for accountability. The Court of Appeal held that the deployment of facial recognition technology infringed privacy rights, owing to inadequate safeguards and the absence of sufficient clarity governing its use and operation.

E. Security Vulnerabilities

The ability of the AI system to centralize vast datasets for ADM creates a prime target for cyberattacks, causing personal data violation and inversion attacks.

IV. THE GDPR AND THE REGULATION OF AUTOMATED DECISION-MAKING

The General Data Protection Regulation constitutes a comprehensive regulatory framework designed to respond to the complexities introduced by contemporary data processing technologies. It articulates a series of core principles that govern the handling of personal data, including lawfulness, fairness, purpose limitation, transparency, and accountability, all of which bind data controllers and processors. In particular, the principle of purpose limitation requires that personal data be collected for clearly defined, legitimate purposes, and that individuals be adequately informed of those purposes at the point of collection. The framework further demands that data be processed in a fair manner and in strict compliance with applicable data protection rules. Under the principle of storage limitation, personal data must not be retained beyond the period necessary to achieve the purpose for which it was collected, and should be erased once that purpose has been fulfilled. Additionally, the principle of data minimization obliges organizations to limit data collection to what is strictly necessary for the intended processing activity.

These principles are intended to ensure that data processing activities respect individuals' rights and are subject to appropriate safeguards.

A. Article 22 GDPR and Automated Decision-Making

A particularly important provision of the General Data Protection Regulation in the context of artificial intelligence is Article 22, which confers on individuals the right not to be subjected to decisions based exclusively on automated processing where such decisions produce legal consequences or similarly significant effects. However, this safeguard is not absolute, as it admits certain exceptions, including circumstances in which the processing is necessary for the performance of a contract or is expressly authorized by law. The interpretation of Article 22 has been the subject of considerable debate. In Schufa Holding AG, the CJEU addressed the application of automated decision-making in the context of credit scoring. The Court emphasized the need for transparency and safeguards but also highlighted the complexity of applying these principles in practice.

B. Transparency and the Right to Explanation

The General Data Protection Regulation imposes an obligation on organizations to furnish

individuals with meaningful information concerning the logic underpinning automated decision-making processes. This has been interpreted by some scholars as establishing a right to explanation. However, the practical implementation of this right remains contested. As watcher and others have argued, the GDPR does not explicitly provide a fully developed right to explanation, and the complexity of AI systems may make meaningful explanations difficult to achieve.

Limitations of the GDPR

Despite its strengths, the GDPR faces several limitations in addressing AI-related risks. These include:

- Difficulties in enforcing transparency obligations
- Limited applicability to non-personal data
- Variations in enforcement across Member States

These limitations highlight the need for complementary regulatory approaches.

V. THE EU ARTIFICIAL INTELLIGENCE ACT: A STRUCTURAL SHIFT IN REGULATION

The EU Artificial Intelligence Act is seen as the first comprehensive legal framework for AI, the act implements strict governance, risk management and transparency requirements for the deployment of AI system in the processing of data.

A. From Data Protection to System Regulation

While the GDPR focuses primarily on the processing of personal data, the EU Artificial Intelligence Act (AI Act) represents a broader regulatory shift towards governing the design, development, and deployment of AI systems themselves. The EU AI Act is particularly enacted for the purpose of regulating the operation of Artificial Intelligence technologies. This distinction is critical, as many of the risks posed by AI arise not merely from data processing but from the architecture and functioning of algorithmic systems.
The AI Act introduces a risk-based regulatory model, categorizing AI systems into four levels: unacceptable risk, high-risk, limited risk, and minimal risk. Systems deemed to pose an "unacceptable risk," such as certain forms of social scoring, are prohibited outright. High-risk systems; those systems used in areas such as employment, credit scoring, education, and law enforcement are subject to stringent regulatory requirements. This approach reflects a preventive logic: rather than addressing harms after they occur, the AI Act seeks to mitigate risks at the design stage.

B. Obligations for High-Risk AI Systems

Under the EU AI Act, high-risk AI systems must comply with a range of obligations, including:

a. Robust data governance and quality standards
b. Maintenance of comprehensive technical documentation and systematic record-keeping
c. Compliance with applicable transparency obligations

d. Implementation of effective human oversight measures
e. Assurance of accuracy, robustness, and appropriate cybersecurity protections.

These requirements aim to ensure that AI systems operate in a manner consistent with fundamental rights, including privacy rights.

The requirement for meaningful human oversight is very important, because it seeks to prevent fully autonomous decision-making in high-stakes contexts. This provision responds directly to concerns raised under the GDPR regarding the limitations of Article 22.

C. Complementarity with the GDPR

The interaction between the General Data Protection Regulation and the Artificial Intelligence Act should be viewed as complementary rather than hierarchical, with the GDPR providing the regulatory framework for the processing of personal data, while the AI Act regulates the systems that process that data. However, this dual framework raises important questions about regulatory coherence. In practice, organizations deploying AI systems must navigate both regimes, potentially leading to overlaps, gaps, and inconsistencies.

For example, a system may comply with the technical requirements of the AI Act while still violating GDPR principles such as data minimization, accountability or purpose limitation. This highlights the need for greater alignment between the two frameworks.

D. Limitations of the AI Act

Despite the innovative approach of the EU AI Act, the EU AI Act is not without its shortcomings. First, its focus on risk classification may lead to under-regulation of systems that fall outside the "high-risk" category but still pose significant privacy concerns.
Second, the Act imposes primary responsibility on developers and providers, potentially overlooking the role of deplorers and users in generating harms.

Third, the AI Act does not create strong, directly enforceable rights for individuals comparable to those under the GDPR. This limits its capacity to serve as a rights-based instrument.

Finally, the complexity of the regulatory framework may pose challenges for implementation, particularly for smaller organizations.

VI. Algorithmic Opacity and Accountability: the Persistence of the Black-Box Problem

Algorithmic Opacity refers to the "black-box" nature of complex AI technologies where decision-making processes are not open, creating challenges in accountability. Accountability is a key principle of data protection which ensures that companies are held liable for AI-driven harms. Solving this challenge requires transparency, explain ability, and audits. Despite regulatory efforts, algorithmic opacity remains a central challenge in AI governance. Many machine learning systems operate through complex statistical

models that are not easily interpretable. This opacity has significant legal implications. Without understanding how a decision is made, individuals cannot effectively exercise their rights to challenge or appeal that decision.

The limitations of transparency requirements are evident in practice. Even where organizations provide information about their systems, such information may be too technical or abstract to be meaningful.

Major Aspects of Algorithmic Opacity

- Technical Complexity: this involves the advanced machine-learning models, especially neutral networks, which are often too complex for humans to understand how it functions to produce results.
- Commercial Secrecy: algorithms are usually viewed as proprietary intellectual property preventing scrutiny and stopping independent auditing.
- Data problems: opacity can come from biased or opaque training data, resulting to hidden discrimination.

A. The Limits of the "Right to Explanation"

The idea of a "right to explanation" has been widely discussed in the context of AI regulation. However, as scholars such as Wachter, Mittelstadt, and Floridi have argued, the GDPR does not provide a fully developed right to explanation.

Moreover, even if such a right were clearly established, its practical implementation would face significant challenges. Complex AI systems may not produce explanations in a form that is easily understandable, raising questions about the feasibility of meaningful transparency.

B. Accountability Beyond Transparency

Given these limitations, there is increasing recognition that transparency alone is insufficient. Instead, a broader framework of accountability is required. This includes:

a. Independent auditing of AI systems
b. Regulatory oversight mechanisms
c. Impact assessments and risk evaluations
d. Clear allocation of responsibility among actors

The concept of algorithmic accountability emphasizes that organizations should be responsible not only for the outcomes of AI systems but also for the processes through which those outcomes are generated.

VII. CONCLUSION

Artificial intelligence poses both a transformative potential and a substantial challenge for contemporary legal systems. Its ability to influence decision-making processes carries significant consequences for the safeguarding of privacy and other fundamental rights. The General Data Protection Regulation and the Artificial Intelligence Act constitute key regulatory landmarks, collectively establishing a framework to mitigate the risks arising

from automated decision-making. However, as this article has demonstrated, significant gaps remain. Challenges such as algorithmic opacity, limited transparency, and fragmented regulatory approaches continue to undermine effective protection.

Addressing these challenges requires a more integrated, rights-cantered approach to regulation, one that places individuals at the heart of AI governance. Only through such an approach can the benefits of AI be realized without compromising the fundamental values that underpin democratic societies.

RECOMMENDATIONS

Need for Harmonized and Rights-Cantered Framework: Integrating GDPR and AI Act Principles: A key challenge in AI regulation is the need to integrate different legal frameworks into a coherent system. This requires aligning the principles of the GDPR with the risk-based approach of the AI Act. Such integration would ensure that both data protection and system design considerations are addressed.

Strengthening Transparency and Explain ability: Regulatory frameworks should move beyond formal transparency requirements to ensure that individuals receive meaningful and accessible explanations. This may involve:

i. Simplified explanation models
ii. User-friendly disclosures
iii. Standardized reporting formats

Enhancing Human Oversight: Human oversight should be more than a formal requirement. It must involve genuine capacity to intervene, review, and override decisions.
Improving Enforcement Mechanisms: Effective regulation requires strong enforcement. This includes:

- Adequate resources for regulatory authorities
- Clear penalties for non-compliance
- Cross-border cooperation

Advancing Ethical Oversight of AI: Legal regulations ought to be reinforced by ethical standards that emphasize fairness, accountability, and the protection of human dignity.

REFERENCES

[1] Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work and Think (John Murray 2013)
[2] Alan F Westin, Privacy and Freedom (Atheneum 1967)
[3] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015)
[4] Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books 2019)
[5] Mireille Hildebrandt, Smart Technologies and the End(s) of Law (Edward Elgar 2015)

[6] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193
[7] Paul M Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 Harvard Law Review 2056
[8] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701
[9] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7 International Data Privacy Law 76
[10] Karen Yeung, 'A Study of the Implications of Advanced Digital Technologies' (2018)
[11] Sylvia Lu, 'Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence' (2020) 23 Vanderbilt Journal of Entertainment and Technology Law https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/3 accessed 20 February 2026
[12] [CASE] Katz v United States 389 US 347 (1967)
[13] [CASE] Campbell v MGN Ltd [2004] UKHL 22, [2004] 2 AC 457
[14] [CASE] Digital Rights Ireland Ltd v Minister for Communications (Joined Cases C 293/12 and C 594/12) EU:C:2014:238
[15] [CASE] State v Loomis 881 NW 2d 749 (Wis 2016)
[16] [CASE] R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058
[17] [CASE] SCHUFA Holding AG (Case C 634/21) EU:C:2023:957
[18] Regulation (EU) 2016/679 (General Data Protection Regulation) ('GDPR'), arts 4(4), 5, 13–15, 22
[19] European Commission, Proposal for an Artificial Intelligence Act COM(2021) 206 final
[20] Sandra Wachter, Brent Mittelstadt and Luciano Floridi (n 20)