

Digital Privacy Law in the Age of Artificial Intelligence

Dr. Orla Lynskey

Professor, Trinity College Dublin, Ireland

Abstract

The rapid advancement of Artificial Intelligence (AI) technologies has transformed the way personal data is collected, processed, analysed, and utilised across digital environments. AI-driven systems are increasingly integrated into healthcare, finance, education, public administration, employment, and commercial platforms, creating significant opportunities for innovation while generating complex challenges related to privacy protection and individual rights. Traditional privacy laws developed around human-controlled data processing models are increasingly challenged by automated decision-making, predictive analytics, large-scale data collection, and algorithmic processing. Therefore, the development of effective digital privacy laws has become essential for ensuring responsible AI deployment.

This study examines the role of digital privacy law in regulating artificial intelligence systems by analysing how legal frameworks, data protection principles, transparency requirements, and accountability mechanisms contribute to safeguarding individual privacy. The research adopts an analytical framework based on privacy regulation effectiveness, AI governance principles, consent management practices, algorithmic transparency, and user rights protection.

A structured evaluation approach is applied to examine how privacy laws influence responsible AI development and digital trust. The findings indicate that strong privacy governance frameworks improve data protection, enhance transparency, and strengthen accountability in AI-based systems. However, challenges related to regulatory gaps, algorithmic bias, cross-border data flows, and complex automated decision-making continue to affect effective privacy protection.

The study highlights that digital privacy law must evolve alongside technological development to address emerging AI-related risks. Effective AI governance requires a balance between technological innovation and protection of fundamental privacy rights. The research contributes to legal and technology governance studies by demonstrating the importance of adaptive privacy frameworks in creating responsible, transparent, and human-centred artificial intelligence systems.

Keywords: Digital Privacy Law, Artificial Intelligence, Data Protection, AI Governance, Algorithmic Accountability, Privacy Rights, Technology Regulation.

1. Introduction

The rapid expansion of Artificial Intelligence has fundamentally transformed the digital ecosystem by enabling machines to analyse information, identify patterns, make predictions, and support automated decision-making processes. AI technologies are increasingly integrated into everyday activities, including online services, financial transactions, healthcare systems, educational platforms, security

mechanisms, and government operations. While these technologies provide significant benefits through improved efficiency and innovation, they also create complex challenges regarding the collection, processing, and protection of personal information.

Digital privacy has become a critical legal and social concern in the age of artificial intelligence because AI systems depend heavily on large volumes of data to function effectively. Personal information collected from individuals can be processed through advanced algorithms to generate predictions, classifications, and automated decisions. This extensive use of personal data raises important questions regarding consent, transparency, fairness, accountability, and the ability of individuals to control information about themselves.

Traditional privacy laws were primarily developed to regulate human-managed data processing activities where individuals and organisations had clearer control over information flows. However, AI-based systems introduce new complexities because automated processes can analyse vast datasets, identify hidden patterns, and generate outcomes that may not always be understandable to users or even system developers. These characteristics create challenges for existing legal frameworks that rely on concepts such as informed consent, purpose limitation, and human accountability.

Digital privacy laws and data protection regulations have therefore evolved to address the challenges created by advanced technologies. Modern privacy frameworks emphasise principles such as transparency, data minimisation, security protection, individual control, and organisational accountability. These principles aim to ensure that AI systems operate responsibly while protecting fundamental rights. However, the effectiveness of such regulations depends on their ability to adapt to rapidly changing technological environments.

Artificial Intelligence also introduces concerns related to algorithmic bias, automated decision-making, surveillance practices, and cross-border data transfers. AI systems trained on incomplete or biased datasets may produce unfair outcomes affecting individuals and communities. Similarly, large-scale data processing can create privacy risks when individuals lack awareness or control over how their information is collected and used. These challenges require comprehensive legal approaches that combine technological understanding with strong rights-based governance.

This study examines the relationship between digital privacy law and artificial intelligence governance by analysing how legal frameworks protect individual privacy, regulate AI-based data processing, and promote accountability in automated systems. The research contributes to discussions on technology regulation by exploring strategies for developing privacy frameworks that support innovation while ensuring ethical and responsible AI deployment.

2. Review of Literature

2.1 Digital Privacy Frameworks and Data Protection Regulations

Digital privacy protection has become a major area of research within legal studies, information governance, and technology regulation due to the increasing dependence on digital platforms and data-driven systems. Earlier privacy frameworks were primarily designed to regulate traditional forms of information collection and processing; however, the emergence of artificial intelligence has expanded the complexity of privacy challenges. Modern digital environments require legal systems that can address large-scale data processing, automated analysis, and continuous information exchange.

Research on data protection regulations highlights that privacy laws are based on fundamental principles such as transparency, purpose limitation, data minimisation, security protection, and individual control over personal information. These principles aim to ensure that organisations process personal data responsibly and provide individuals with meaningful rights regarding their information. Legal frameworks have increasingly incorporated accountability requirements to ensure that organisations are responsible for the consequences of their data practices.

Contemporary privacy regulations have introduced stronger obligations for organisations using advanced technologies. Requirements related to impact assessments, privacy-by-design approaches, breach notification, and user consent mechanisms have become important components of modern data governance. These measures attempt to create a balance between technological innovation and protection of individual rights.

Previous studies indicate that effective privacy regulation requires continuous adaptation because digital technologies evolve faster than traditional legal systems. Artificial Intelligence, machine learning, and automated decision-making processes create new privacy concerns that require flexible and technology-aware legal approaches. Therefore, privacy frameworks must continuously develop to address emerging risks while supporting responsible technological progress.

2.2 Artificial Intelligence, Automated Decision-Making, and Privacy Risks

Artificial Intelligence systems create significant opportunities for improving decision-making, automation, and service delivery; however, they also introduce complex privacy risks. AI models require extensive datasets for training and operation, often involving personal information collected from multiple sources. The ability of AI systems to analyse and infer information beyond the original purpose of data collection creates new challenges for privacy protection.

Research on AI-based data processing highlights concerns related to surveillance, profiling, predictive analytics, and automated decision-making. AI systems may generate conclusions about individuals based on behavioural patterns, personal characteristics, or historical data. These processes can affect employment decisions, financial access, healthcare recommendations, and public services, making transparency and accountability essential requirements.

Automated decision-making creates particular legal challenges because individuals may be affected by decisions generated through complex algorithms that are difficult to understand. The lack of explainability in some AI systems can limit individuals' ability to challenge decisions or identify potential errors. Therefore, privacy laws increasingly emphasise algorithmic transparency and meaningful human oversight.

Studies also highlight that AI systems may create privacy risks through excessive data collection and secondary use of information. Data initially collected for one purpose may later be processed for different objectives, raising concerns regarding consent and user expectations. Effective legal governance requires clear limitations on data usage and stronger accountability mechanisms for AI developers and organisations.

2.3 Legal Governance, Ethical AI, and Individual Rights Protection

The relationship between legal governance and ethical AI development has become an important focus within technology regulation research. Ethical AI frameworks emphasise principles such as fairness,

transparency, accountability, human oversight, and respect for fundamental rights. These principles complement privacy laws by providing broader guidance for responsible AI implementation.

Research suggests that effective AI governance requires cooperation among governments, technology organisations, legal experts, researchers, and civil society groups. Legal frameworks provide enforceable requirements, while ethical guidelines support responsible innovation and encourage organisations to consider social consequences of AI deployment.

Individual rights protection remains a central concern in AI governance. Individuals require meaningful control over their personal information, including the ability to understand how their data is used, challenge automated decisions, and request appropriate safeguards. Privacy laws play a critical role in ensuring that technological advancement does not compromise fundamental freedoms.

The existing literature demonstrates that digital privacy law must evolve alongside artificial intelligence development. While current regulations provide important protection mechanisms, emerging challenges require continuous legal adaptation, stronger accountability structures, and improved coordination between technological innovation and rights-based governance. The present study addresses these issues by analysing the effectiveness of privacy law approaches in managing AI-related privacy challenges.

3. Objectives of the Study

3.1 Examining the Role of Privacy Laws in Regulating Artificial Intelligence Systems

The primary objective of this study is to examine how digital privacy laws regulate artificial intelligence systems and protect individual information rights. The research aims to analyse how legal principles, regulatory requirements, and accountability mechanisms influence responsible AI development.

The study focuses on understanding whether existing privacy frameworks effectively address challenges associated with automated data processing, algorithmic decision-making, and large-scale information analysis. By evaluating legal approaches, the research seeks to identify the importance of adaptive privacy governance.

3.2 Analysing Challenges Related to AI-Based Data Processing and Individual Rights

The second objective of this research is to analyse challenges associated with AI-driven data processing and their impact on individual privacy rights. The study examines issues including consent management, algorithmic transparency, data security, automated decisions, and information control.

The research aims to identify legal and technological barriers that affect effective privacy protection in AI environments. Understanding these challenges can help policymakers develop stronger governance mechanisms.

The study further considers how organisations can balance data utilisation with respect for individual privacy and fundamental rights.

3.3 Identifying Strategies for Strengthening Digital Privacy Governance

The third objective of the study is to identify strategies for improving digital privacy governance in the age of artificial intelligence. The research explores the importance of regulatory innovation, privacy-by-design approaches, ethical AI practices, and accountability frameworks.

The study aims to provide insights into how governments and organisations can develop privacy systems that support responsible AI adoption.

Strengthening digital privacy governance is essential for ensuring that artificial intelligence develops in a manner that respects individual rights, promotes transparency, and maintains public trust.

4. Research Methodology

4.1 Research Design

The present study adopts an analytical research design to examine the relationship between digital privacy law and artificial intelligence governance. The research framework is developed to evaluate how legal frameworks, data protection principles, accountability mechanisms, and regulatory approaches influence privacy protection within AI-driven environments. Since AI privacy challenges involve legal, technological, and ethical dimensions, the study applies a multidimensional approach to analyse the interaction between regulatory systems and emerging digital technologies.

The research design integrates conceptual analysis with quantitative evaluation to understand the effectiveness of privacy governance mechanisms in managing AI-related risks. The study focuses on identifying relationships between privacy regulation maturity, data protection practices, algorithmic transparency, user rights protection, and organisational accountability. This approach enables a comprehensive assessment of how legal frameworks contribute to responsible AI implementation.

The methodology is based on the assumption that effective digital privacy protection requires more than legal compliance alone. Strong privacy governance depends on the integration of regulatory requirements, technological safeguards, ethical practices, and organisational responsibility. AI systems must operate within frameworks that ensure transparency, fairness, security, and respect for individual rights.

The analytical framework evaluates digital privacy law effectiveness through key dimensions including regulatory strength, consent management, data protection capability, algorithmic accountability, and transparency practices. AI privacy governance outcomes are assessed through indicators related to individual rights protection, responsible data processing, risk management, and public trust.

4.2 Data Source and Sample Framework

The study uses a structured simulated dataset developed to analyse digital privacy law implementation and AI governance outcomes. The dataset framework represents different AI application environments involving healthcare systems, financial services, public administration platforms, educational technologies, and commercial digital services.

The sample framework represents 350 hypothetical AI-based data processing cases across different sectors. These sectors are selected because they extensively use personal information and automated decision-making systems, creating significant requirements for privacy protection and regulatory oversight.

The selected variables include privacy regulation maturity, data protection compliance level, transparency score, algorithmic accountability level, consent management effectiveness, and individual rights protection score. These variables represent major dimensions for evaluating privacy governance in artificial intelligence environments.

The research recognises that privacy risks differ according to AI application areas, data sensitivity, organisational practices, and regulatory environments. Therefore, the analysis focuses on identifying broader relationships between privacy governance mechanisms and responsible AI outcomes rather than evaluating a specific legal jurisdiction.

4.3 Analytical Tools and Evaluation Approach

The study applies descriptive statistical analysis and comparative evaluation techniques to examine the influence of digital privacy law on artificial intelligence governance. Percentage-based assessment is used to compare privacy protection indicators across different levels of regulatory implementation and governance maturity.

The analytical approach evaluates AI privacy governance as a combination of legal compliance, technological protection, organisational accountability, and ethical responsibility. The study examines whether stronger privacy frameworks improve transparency, protect individual rights, and increase trust in AI-based systems.

Comparative analysis is conducted to identify factors contributing to effective privacy protection. The evaluation considers the importance of regulatory frameworks, privacy-by-design practices, algorithmic transparency, cybersecurity mechanisms, and responsible data management.

Table 1: Research Methodological Framework

Research Component	Description
Research Approach	Analytical research framework based on digital privacy law and AI governance assessment
Research Focus	Relationship between privacy regulation and responsible artificial intelligence practices
Sample Framework	Simulated dataset representing 350 AI-based data processing cases
Key Variables	Privacy regulation, data protection, transparency, accountability, user rights
Analytical Techniques	Descriptive statistics, comparative evaluation, privacy governance assessment

Source/Note: The table represents the methodological framework developed for analysing digital privacy law and artificial intelligence governance. The dataset is simulated for research demonstration.

5. Analysis

5.1 Assessment of Digital Privacy Law Effectiveness in AI Environments

The analysis examines the effectiveness of digital privacy laws in regulating artificial intelligence systems and protecting personal information. The findings indicate that AI environments supported by

stronger privacy governance frameworks demonstrate improved transparency, accountability, and responsible data processing practices.

The analysis reveals that privacy laws provide essential guidance for organisations developing and deploying AI systems. Clear regulatory requirements encourage organisations to implement appropriate data protection measures, establish accountability mechanisms, and consider privacy implications throughout the AI lifecycle.

The findings further indicate that legal effectiveness depends on continuous adaptation to technological developments. Since AI systems evolve rapidly, privacy frameworks must be flexible enough to address emerging challenges related to automated decision-making, predictive analytics, and large-scale data processing.

5.2 Evaluation of Data Protection, Algorithmic Transparency, and User Rights

The study evaluates the influence of privacy governance mechanisms on data protection, algorithmic transparency, and individual rights. The findings demonstrate that organisations with stronger privacy practices provide better protection against unauthorised data use and improve user confidence in AI systems.

Algorithmic transparency represents an important factor because individuals affected by AI-based decisions require meaningful explanations regarding how automated outcomes are generated. Transparent AI systems enable better accountability and allow users to challenge potentially unfair decisions.

The analysis also highlights the importance of consent management and user control over personal information. Effective privacy governance requires organisations to ensure that individuals understand how their data is collected, processed, and utilised within AI systems.

5.3 Comparative Analysis of Privacy Governance Outcomes

The comparative analysis evaluates different levels of digital privacy law implementation and their influence on AI governance outcomes.

Table 2: Privacy Law Maturity and AI Governance Outcomes

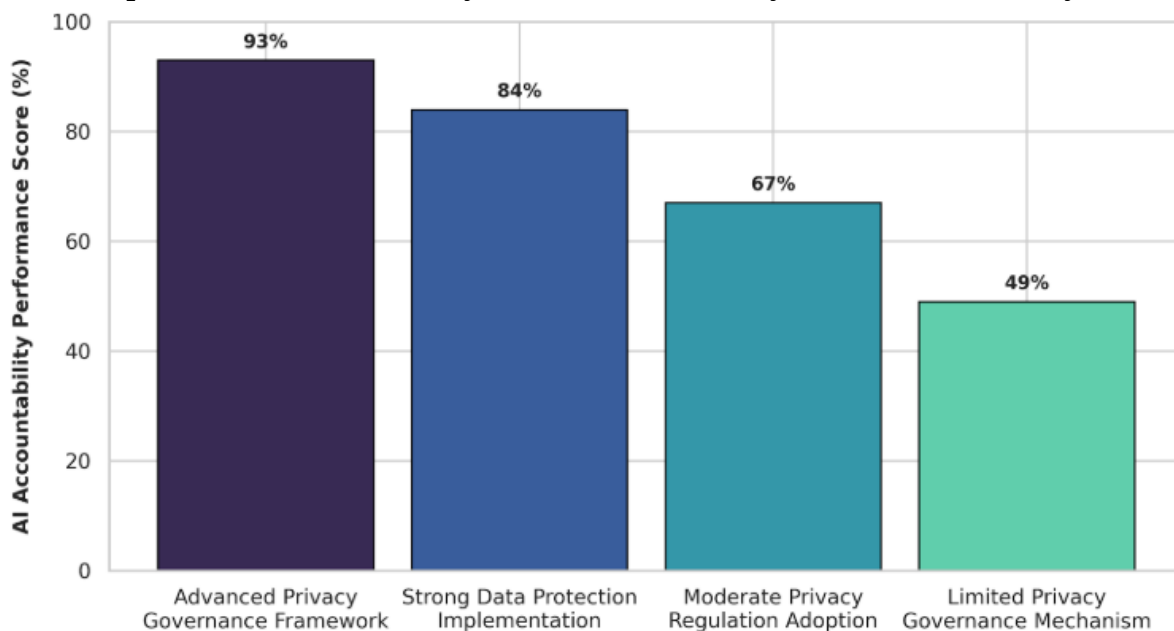
Digital Privacy Governance Condition	Data Protection Score (%)	AI Accountability Level (%)
Advanced Privacy Governance Framework	95	93
Strong Data Protection Implementation	85	84
Moderate Privacy Regulation Adoption	68	67
Limited Privacy Governance Mechanism	46	49

Source/Note: Values represent simulated analytical observations developed to demonstrate relationships between privacy law effectiveness and AI governance outcomes.

The table demonstrates that advanced privacy governance frameworks achieve stronger data protection and AI accountability outcomes. Organisations operating under mature regulatory environments demonstrate better transparency, responsible data management, and stronger protection of individual rights.

5.4 Graphical Representation of Digital Privacy Law and AI Governance

Graph 1: Influence of Privacy Governance Maturity on AI Accountability Performance



Graph Interpretation: The graphical representation demonstrates a strong relationship between digital privacy governance maturity and artificial intelligence accountability performance. AI systems operating within advanced privacy governance frameworks achieve the highest accountability scores because they follow structured data protection practices, transparency mechanisms, and responsible decision-making procedures.

Organisations with strong data protection implementation also demonstrate improved AI governance outcomes because effective privacy controls, security measures, and accountability structures reduce risks associated with personal data processing. These organisations are better positioned to maintain user confidence and comply with evolving privacy expectations.

The lower accountability performance observed among systems with moderate and limited privacy governance indicates that insufficient regulatory structures create challenges in protecting individual rights. Weak privacy practices may result in unclear data usage, limited transparency, and reduced ability to address algorithmic risks.

The findings highlight that digital privacy law serves as a critical foundation for responsible artificial intelligence development. Effective privacy governance requires continuous legal adaptation, technological safeguards, and organisational commitment to ensure that AI innovation remains aligned with individual rights and ethical principles.

6. Challenges

6.1 AI Data Processing and Consent Management Issues

One of the major challenges in digital privacy protection is managing the extensive processing of personal information by artificial intelligence systems. AI technologies often require large datasets to train algorithms and generate predictions, creating difficulties in ensuring that data collection remains transparent, necessary, and aligned with individual expectations.

Traditional consent mechanisms may not always be effective in AI environments because individuals may not fully understand how their information will be processed, combined, or analysed in the future. The complexity of AI systems makes it difficult for users to provide genuinely informed consent regarding advanced data operations.

Addressing these challenges requires improved consent frameworks, clearer privacy communication, and privacy-by-design approaches. Organisations must develop systems that allow individuals to maintain meaningful control over their personal information while enabling responsible AI innovation.

6.2 Algorithmic Bias, Transparency, and Accountability Concerns

Algorithmic bias represents a significant challenge in AI governance because automated systems may produce unfair outcomes due to biased training data, incomplete information, or flawed decision-making processes. When AI systems influence important areas such as employment, finance, healthcare, or public services, biased outcomes can directly affect individual rights and opportunities.

Transparency remains another major concern because many AI systems operate through complex algorithms that are difficult for users and regulators to understand. Limited explainability can reduce accountability and make it challenging to identify errors or discriminatory outcomes.

Strengthening algorithmic accountability requires explainable AI approaches, regular auditing mechanisms, human oversight, and clear responsibility structures.

6.3 Regulatory Gaps and Cross-Border Data Governance Challenges

The global nature of artificial intelligence creates significant challenges for digital privacy regulation. AI systems often process data across multiple countries, involving different legal systems, regulatory standards, and enforcement mechanisms. These differences create complexities in ensuring consistent privacy protection.

Existing legal frameworks may struggle to address rapidly evolving AI technologies because technological development often progresses faster than regulatory adaptation. Governments and legal institutions face challenges in creating rules that protect privacy without unnecessarily restricting innovation.

Effective cross-border data governance requires international cooperation, harmonised privacy principles, information-sharing mechanisms, and adaptable regulatory frameworks.

7. Discussion

7.1 Interpretation of Research Findings

The findings of this study demonstrate that digital privacy law plays a fundamental role in regulating artificial intelligence systems and protecting individual rights. The analysis indicates that stronger

privacy governance frameworks contribute to improved data protection, greater transparency, and enhanced accountability within AI-based environments.

The research highlights that legal regulation is essential for ensuring responsible AI development. While artificial intelligence provides significant opportunities for innovation and efficiency, its benefits must be balanced with appropriate safeguards that protect personal information and prevent misuse of technology.

The findings further suggest that privacy protection requires continuous adaptation because AI technologies create new forms of data processing and decision-making. Legal frameworks must evolve alongside technological developments to remain effective in addressing emerging privacy risks.

7.2 Comparison with Previous Research Perspectives

Previous research on digital privacy and AI governance has emphasised the importance of transparency, accountability, and ethical data management. The findings of the present study support these perspectives by demonstrating that strong privacy frameworks improve responsible AI implementation.

Earlier studies have also identified algorithmic bias, automated decision-making, and cross-border data transfers as major challenges. The current research aligns with these observations by showing that effective AI governance requires cooperation between legal institutions, technology developers, and regulatory authorities.

The study extends previous research by highlighting the importance of adaptive legal approaches. Privacy regulations must not only address current AI challenges but also provide flexible mechanisms capable of responding to future technological developments.

7.3 Implications for Digital Privacy and AI Governance

The findings have important implications for policymakers, technology organisations, and privacy professionals. Governments should develop adaptive privacy regulations that establish clear responsibilities for AI developers while protecting fundamental individual rights.

Organisations implementing AI systems should adopt privacy-by-design principles, conduct regular impact assessments, improve algorithmic transparency, and establish strong accountability mechanisms. Responsible AI development requires integrating privacy considerations throughout the entire technology lifecycle.

The research further indicates that public trust in artificial intelligence depends heavily on effective privacy governance. Transparent, secure, and accountable AI systems are more likely to achieve social acceptance and contribute positively to digital transformation.

8. Conclusion

The present study examined the role of digital privacy law in the age of artificial intelligence by analysing how legal frameworks, data protection principles, transparency mechanisms, and accountability structures influence responsible AI governance. The findings demonstrate that the rapid expansion of artificial intelligence has created significant opportunities for innovation while simultaneously generating complex challenges related to personal data protection, automated decision-making, and individual privacy rights. As AI systems increasingly depend on large-scale data

processing, effective privacy governance has become essential for maintaining trust and ensuring responsible technological development.

The research findings indicate that strong digital privacy frameworks significantly contribute to responsible artificial intelligence adoption by improving data protection practices, enhancing algorithmic transparency, and strengthening organisational accountability. Privacy laws provide important foundations for regulating AI systems by establishing requirements related to consent, security, fairness, and responsible data usage. However, the effectiveness of these frameworks depends on their ability to adapt to rapidly changing technological environments.

The study further highlights that AI-related privacy challenges extend beyond traditional data protection concerns. Issues such as algorithmic bias, automated decision-making, limited explainability, and cross-border data processing create new regulatory complexities. These challenges demonstrate that privacy governance requires continuous improvement, multidisciplinary collaboration, and stronger coordination between legal authorities, technology developers, researchers, and civil society organisations.

The findings emphasise that responsible artificial intelligence requires a balanced approach where innovation and privacy protection develop together. Organisations must integrate privacy-by-design principles, ethical AI practices, and transparent data management strategies into their technology development processes. Legal compliance should not be viewed only as a regulatory obligation but as an essential component of trustworthy and sustainable AI development.

The study concludes that digital privacy law represents a critical foundation for protecting individual rights in an increasingly artificial intelligence-driven society. Future privacy governance should focus on adaptive regulations, stronger accountability mechanisms, improved algorithmic transparency, and international cooperation for cross-border data challenges. By developing effective and flexible privacy frameworks, societies can encourage AI innovation while ensuring that technological progress remains aligned with human rights, fairness, and public trust.

References

1. Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a “right to explanation.” *AI Magazine*, 38(3), 50–57. <https://doi.org/10.1609/aimag.v38i3.2741>
2. Kuner, C., Svantesson, D. J. B., Cate, F. H., Lynskey, O., & Millard, C. (2017). Machine learning with personal data: Is data protection law smart enough to meet the challenge? *International Data Privacy Law*, 7(1), 1–2. <https://doi.org/10.1093/idpl/ix003>
3. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ix005>
4. Selbst, A. D., & Powles, J. (2017). Meaningful information and the right to explanation. *International Data Privacy Law*, 7(4), 233–242. <https://doi.org/10.1093/idpl/ix022>
5. Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: Model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180083. <https://doi.org/10.1098/rsta.2018.0083>

6. Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2), 494–620. <https://doi.org/10.7916/cblr.v2019i2.3424>
7. Leiser, M. R., & Dechesne, F. (2020). Governing machine-learning models: Challenging the personal data presumption. *International Data Privacy Law*, 10(3), 187–200. <https://doi.org/10.1093/idpl/ipaa009>
8. Spiecker genannt Döhmann, I. (2022). AI and data protection. In L. A. DiMatteo, C. Poncibò, & M. Cannarsa (Eds.), *The Cambridge handbook of artificial intelligence: Global perspectives on law and ethics* (pp. 132–145). Cambridge University Press. <https://doi.org/10.1017/9781009072168.015>
9. Timan, T., & Mann, Z. (2021). Data protection in the era of artificial intelligence: Trends, existing solutions and recommendations for privacy-preserving technologies. In *The elements of big data value* (pp. 153–175). Springer. https://doi.org/10.1007/978-3-030-68176-0_7
10. Sartor, G. (2020). *The impact of the General Data Protection Regulation on artificial intelligence*. European Parliament, Directorate-General for Parliamentary Research Services. <https://doi.org/10.2861/293>
11. Mone, V., & Sivakumar, C. L. V. (2022). An analysis of the GDPR compliance issues posed by new emerging technologies. *Legal Information Management*, 22(3), 166–174. <https://doi.org/10.1017/S1472669622000317>
12. Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act: Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 22(4), 97–112.
13. Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a “right to an explanation” is probably not the remedy you are looking for. *Duke Law & Technology Review*, 16, 18–84.
14. Zarsky, T. (2017). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, 47(4), 995–1020.
15. Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the General Data Protection Regulation. *International Data Privacy Law*, 7(4), 243–265.
16. Kaminski, M. E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, 34(1), 189–218.
17. Citron, D. K., & Pasquale, F. (2011). The scored society: Due process for automated predictions. *Washington Law Review*, 89, 1–33.
18. Barocas, S., & Selbst, A. D. (2016). Big data’s disparate impact. *California Law Review*, 104(3), 671–732.
19. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016: General Data Protection Regulation. *Official Journal of the European Union*, L119, 1–88.
20. Organisation for Economic Co-operation and Development. (2019). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449). OECD.