

Artificial Intelligence and the Future of Subject Access Request: Transforming Data Disclosure Under the Uk GDPR

Temitope Olodo

Department of Political Science
Usmanu Danfodio University, Sokoto, Nigeria
Email: yolodo@yahoo.com
ORCID: <https://orcid.org/0009-0007-6538-2694>

Mudassir Nasir, Ph.D.

Department of Criminology and Security Studies
Iconic Open University
Mobile No.: +2348032915882
ORCID: <https://orcid.org/0009-0003-2378-627X>
Email: mudassirnasir1996@gmail.com | m.nasir@iconicuniversity.edu.ng

Adebimpe Saheed Fagbemi, Ph.D.

Department of Criminology and Forensic Studies
University of Kwa-Zulu Natal, Durban, Republic of South Africa
Email: adebimpefagbemi@yahoo.com
Phone Number: +234 803 408 9692 or +1347 622 7275
ORCID ID: <https://orcid.org/0009-0007-1412-3588>

Muhammad Sani IDRIS

Department of Defence and Security Studies
Faculty of Arts and Social Science,
Nigerian Defence Academy (NDA)
Kaduna- Nigeria.
Email address: sanmuhammadu83@gmail.com
GSM: +2348036654214
ORCID ID: <https://orcid.org/0009-0007-5828-6004>

<https://doi.org/10.56201/wjimt.v10.no8.2026.pg176.195>

Abstract

This article critically examines the transformative impact of Artificial Intelligence (AI) on the administration of Subject Access Requests (SARs) under the United Kingdom General Data Protection Regulation (UK GDPR). As organisations contend with exponential growth in electronically stored information, traditional manual disclosure practices have become increasingly unsustainable. Through doctrinal legal analysis, comparative regulatory research and documentary review, this study evaluates how AI technologies including Large Language Models, Natural Language Processing and semantic search are reshaping SAR administration while assessing the adequacy of existing legal frameworks. The research demonstrates that current UK data protection legislation remains sufficiently adaptable to regulate AI-assisted disclosure through its principles-based approach, though meaningful human oversight remains legally indispensable for interpreting statutory exemptions and balancing competing rights. The study identifies explainability as a defining governance challenge and proposes an original

AI-Augmented Disclosure Governance Framework (AIADGF) integrating legal obligations, organisational governance and AI-enabled technologies into a structured eight-stage model. The framework positions AI as an augmentation of professional legal judgement rather than a replacement, ensuring accountability under Article 5(2) UK GDPR. The article contributes to emerging scholarship at the intersection of AI, information governance and data protection law while offering practical recommendations for policymakers, regulators and organisations seeking to deploy AI responsibly within SAR processes. It concludes that AI should serve as an instrument for strengthening data protection principles through improved transparency, consistency and procedural fairness.

Keywords: Artificial Intelligence, Data Protection, Disclosure Governance, Regulatory Governance Theory (RGT), Subject Access Requests (SARs),

Introduction

The exponential growth of digital information has fundamentally altered the landscape of data protection compliance across both public institutions and private organisations. Every interaction between individuals and organisations now generates significant volumes of electronically stored information (ESI), including emails, messaging applications, cloud-hosted documents, customer relationship management records, CCTV footage, biometric information, call recordings and metadata. This rapid digitalisation has significantly expanded the volume, complexity and diversity of personal data held by organisations, thereby increasing both the frequency and complexity of Subject Access Requests (SARs) submitted under Article 15 of the UK General Data Protection Regulation (UK GDPR; Wolford, 2020).

The right of access is widely regarded as one of the cornerstones of modern data protection law because it enables individuals to understand how organisations collect, process, store and share their personal information. Article 15 UK GDPR provides every data subject with the right to obtain confirmation that their personal data are being processed and, where applicable, to receive access to that information together with supplementary information concerning the purposes of processing, categories of data processed, recipients of the data, retention periods and the existence of automated decision-making processes (UK GDPR, Art. 15). This statutory right is reinforced by the Data Protection Act 2018, which provides the domestic legislative framework governing the exercise of data protection rights within the United Kingdom (Data Protection Act 2018, c. 12). Although the legal principles underpinning Subject Access Requests have remained relatively stable, the operational environment within which organisations respond to those requests has changed dramatically. Two decades ago, disclosure exercises largely involved reviewing paper records or relatively small volumes of electronic correspondence. Today, organisations routinely manage millions of electronic documents dispersed across multiple cloud platforms, mobile devices, enterprise applications and collaborative working environments such as Microsoft Teams, Slack and SharePoint. The sheer scale of contemporary information ecosystems has rendered traditional manual disclosure practices increasingly unsustainable (Bennett & Raab, 2021).

The Information Commissioner's Office (ICO), as the United Kingdom's independent supervisory authority for data protection, has consistently recognised that organisations must adopt effective governance arrangements to ensure compliance with Subject Access Request obligations while maintaining accuracy, proportionality and accountability (Information Commissioner's Office, 2021). ICO guidance emphasises that organisations must conduct reasonable and proportionate searches for personal data and respond without undue delay, normally within one calendar month, subject to limited statutory extensions where requests are particularly complex (Information Commissioner's Office, 2023). However, meeting these

obligations has become increasingly difficult as organisations continue to experience exponential growth in electronically stored information (Millard, 2022).

Artificial Intelligence has emerged as one of the most significant technological developments capable of transforming disclosure management. Unlike conventional search technologies, AI systems can identify patterns, interpret natural language, classify documents according to context, detect duplicates, recognise personal identifiers embedded within unstructured datasets and automate aspects of document review that previously required extensive human intervention (Dale, 2021; Susskind, 2022). Advances in Large Language Models (LLMs), Natural Language Processing (NLP), Optical Character Recognition (OCR), semantic search and machine learning now enable organisations to process substantial quantities of information within significantly shorter timeframes than conventional manual review methods (Vaswani et al., 2017; Zhou et al., 2023).

These technological developments have profound implications for data protection compliance. AI-assisted disclosure promises substantial improvements in efficiency, consistency and cost-effectiveness while reducing the administrative burden associated with responding to increasingly complex Subject Access Requests (Armstrong & Ford, 2023; Buchanan, 2024). Public authorities, healthcare providers, financial institutions and multinational corporations are already exploring AI-enabled document review systems capable of identifying responsive documents, extracting personal information and supporting lawful disclosure decisions (Cabrera & Walker, 2022; Harrington, 2023). The legal technology sector has similarly witnessed significant investment in AI-powered e-disclosure and document review platforms designed to improve litigation disclosure, regulatory investigations and data protection compliance (Katsh & Rabinovich-Einy, 2021).

Nevertheless, the integration of Artificial Intelligence into Subject Access Request administration raises important legal, ethical and governance questions (European Commission, 2021; Yeung, 2023). AI systems are not infallible. Algorithmic bias, inaccurate document classification, excessive redaction, hallucinations generated by Large Language Models and opaque decision-making processes may compromise the rights of data subjects if AI outputs are relied upon without adequate human oversight (Barocas et al., 2019; Wachter et al., 2024). The accountability principle established under Article 5(2) UK GDPR requires controllers not only to comply with data protection principles but also to demonstrate that compliance (UK GDPR, Art. 5(2)). This obligation becomes increasingly complex where AI systems influence decisions concerning the identification, review or disclosure of personal data (Edwards & Veale, 2021).

Furthermore, the UK's evolving regulatory landscape reflects increasing recognition that AI governance and data protection are becoming closely interconnected. Alongside the UK GDPR and the Data Protection Act 2018, the Information Commissioner's Office has published extensive guidance addressing AI, automated decision-making, data protection impact assessments and explainability (Information Commissioner's Office, 2020, 2023). Internationally, the OECD AI Principles, the NIST AI Risk Management Framework, ISO/IEC 42001 Artificial Intelligence Management Systems, and the European Union's AI Act collectively emphasise the importance of transparency, accountability, fairness and human oversight in AI deployment (European Parliament, 2024; ISO, 2023; National Institute of Standards and Technology, 2023; OECD, 2019). These developments suggest that future regulatory expectations concerning AI-assisted disclosure will extend beyond technical efficiency to encompass demonstrable legal compliance and ethical governance (Alston, 2022; Scherer, 2023).

Against this background, this article critically examines how Artificial Intelligence is transforming the administration of Subject Access Requests under the UK GDPR. It evaluates the opportunities presented by AI-assisted disclosure while critically assessing the legal and

regulatory risks associated with automated document review. The study argues that AI should be viewed as an augmentation technology that enhances professional judgement rather than replacing human legal decision-making (Pasquale & Cashwell, 2022; Surden, 2019). To achieve this objective, the article proposes an original AI-Augmented Disclosure Governance Framework (AIADGF) designed to ensure that technological innovation remains compatible with the fundamental rights, procedural safeguards and accountability obligations embedded within UK data protection law (Binns, 2020; Mittelstadt et al., 2023). Through this analysis, the study seeks to contribute to the emerging scholarship at the intersection of Artificial Intelligence, information governance and data protection regulation, while offering practical recommendations for policymakers, regulators, legal practitioners and organisations seeking to deploy AI responsibly within Subject Access Request processes (Crotoft, 2021; Veale & Zuiderveen Borgesius, 2021).

Statement of the Problem

The proliferation of artificial intelligence (AI) is creating a paradoxical crisis for the UK GDPR's right of subject access. While AI empowers data subjects to craft increasingly sophisticated, broad, and voluminous Subject Access Requests (DSARs), it simultaneously overwhelms the very compliance frameworks designed to honour them. This dual pressure exposes a critical legal and operational fault line: the existing statutory framework, even with recent amendments under the Data (Use and Access) Act 2025, struggles to reconcile expansive individual rights with the practical realities of automated data processing.

On one hand, individuals can leverage generative AI to generate complex requests that probe deep into organisational data ecosystems, often demanding granular disclosures that legacy systems cannot efficiently retrieve. On the other hand, controllers face mounting compliance costs, disproportionate effort defences, and regulatory scrutiny as they grapple with deciphering AI-generated requests and locating relevant data across fragmented, algorithmic infrastructures. This tension is exacerbated by the Act's introduction of "reasonable and proportionate search" obligations and "stop the clock" provisions, which, while intended to lighten administrative burdens, introduce new ambiguities regarding the scope of searches and the timelines for responses when AI systems are involved.

Consequently, there exists a significant gap between the legislative intent of empowering data subjects through transparency and the technological reality of fulfilling that right in an AI-driven environment. Without clarity on how AI influences both the demand and supply sides of DSAR compliance, organisations risk either over-disclosing sensitive information or under-fulfilling their legal duties, thereby undermining the very essence of data protection rights. This study examines this transformative friction to propose a sustainable model for AI-augmented DSAR processing.

Research Questions

The study is guided by the following research questions:

- i. How is Artificial Intelligence transforming the administration of Subject Access Requests under the UK GDPR?
- ii. To what extent does the existing legal framework adequately regulate AI-assisted disclosure?
- iii. What legal and ethical challenges arise from the increasing use of Artificial Intelligence in Subject Access Request administration?
- iv. What governance framework can organisations adopt to ensure lawful, transparent and accountable AI-assisted disclosure?

Research Aim and Objectives

Aim: To critically evaluate the regulatory and operational challenges of using Artificial Intelligence in Subject Access Request (SAR) administration under the UK GDPR, and to propose a governance framework for lawful disclosure.

Objectives are to:

- i. Analyse the functional transformation of SAR administration by AI.
- ii. Critically assess the adequacy of the existing UK GDPR and Data Protection Act 2018 framework in regulating the unique risks posed by AI-assisted disclosure
- iii. Identify and examine the legal and ethical tensions arising from AI-assisted SARs, including conflicts between data minimisation and data maximisation, the 'black box' problem in refusal justifications, and the erosion of the right to human intervention.
- iv. Develop a practical, risk-based governance framework that operationalises the principles of lawfulness, transparency, and accountability (Article 5(2) UK GDPR) specifically for organisations deploying AI in the SAR lifecycle.

Literature Review

Conceptualisations

Subject Access Requests (SARs) Through Artificial Intelligence

Subject Access Requests (SARs) Through Artificial Intelligence is situated at the intersection of data protection law, information governance, legal technology and computational intelligence. Understanding this transformation requires an examination of the principal concepts underpinning the legal and technological landscape. This conceptual framework defines the core concepts adopted throughout this study and explains their interrelationship within the administration of Subject Access Requests under the UK General Data Protection Regulation (UK GDPR) (UK GDPR, 2018).

Artificial Intelligence

Artificial Intelligence (AI) refers to computational systems capable of performing tasks that ordinarily require human intelligence, including learning, reasoning, pattern recognition, language interpretation, decision support and predictive analysis (Russell & Norvig, 2021). Unlike traditional software applications that operate solely through predetermined programming instructions, AI systems continuously improve their performance through exposure to data, enabling them to recognise complex relationships and generate contextually relevant outputs. Artificial Intelligence (AI) can be defined as simulation of human intelligence towards development of algorithms and software that enable machines to profile the data of criminal intents, recognize the patterns and nature of the crime, and make decisions based on that learning (Mudassir, 2025).

Within data disclosure, AI extends beyond simple keyword searching by enabling organisations to interpret unstructured information, identify personal data, recognise contextual relationships between documents and recommend disclosure decisions. Contemporary AI technologies increasingly deployed within legal and compliance environments include: Large Language Models (LLMs), Natural Language Processing (NLP), Machine Learning (ML), Optical Character Recognition (OCR), Semantic Search, Named Entity Recognition (NER) and Automated Redaction Technologies. Collectively, these technologies have transformed document review from a largely manual process into one that increasingly relies upon intelligent automation. However, AI should not be understood as a replacement for legal judgement. Instead, it functions as a decision-support technology capable of improving efficiency while requiring continuous human supervision to ensure compliance with statutory obligations (Ashley, 2017).

This study sees Artificial Intelligence (AI) as a computational system capable of performing tasks that ordinarily require human intelligence, including learning, reasoning, pattern recognition, language interpretation, decision support, and predictive analysis. Unlike traditional software that operates through predetermined programming instructions, AI systems continuously improve their performance through exposure to data, enabling them to recognize complex relationships and generate contextually relevant outputs.

Subject Access Requests (SARs)

Subject Access Requests (SARs) constitute one of the fundamental rights conferred upon individuals under Article 15 of the UK GDPR (UK GDPR, 2018). They enable a data subject to obtain confirmation that their personal data are being processed and, where processing occurs, receive access to those data together with supplementary information concerning the purposes of processing, categories of personal data, recipients, retention periods, and safeguards applicable to international transfers (UK GDPR, 2018, Art. 15).

The right of access serves several important objectives. First, it promotes transparency by enabling individuals to understand how organisations process their personal information. Secondly, it facilitates accountability by allowing individuals to challenge inaccurate or unlawful processing. Thirdly, it supports other data protection rights, including rectification, erasure, restriction of processing and objection to processing (Information Commissioner's Office, 2022). In practice, responding to Subject Access Requests often involves searching multiple repositories of electronically stored information, include: Email servers, Cloud storage platforms, Human resource management systems, Customer relationship management databases, CCTV recordings, Instant messaging platforms, Mobile devices, Archived records, Audio recordings and social media communications. Consequently, modern SAR administration has evolved into a sophisticated information retrieval exercise requiring legal interpretation, technological capability and organisational governance.

This study defined Subject Access Request (SARs) as enforceable statutory right of an individual to obtain from an organisation a copy of their personal data, along with comprehensive details of its usage, retention, and sharing. In the era of artificial intelligence and the DUAA 2025, the SAR is evolving from a retrospective data-retrieval tool into a prospective accountability mechanism demanding intelligible explanations of algorithmic logic, compelling proportionate and documented searches, and serving as the central battlefield where individual rights meet automated decision-making.

Data Disclosure

Data disclosure refers to the systematic identification, retrieval, review, redaction and release of personal data to an individual exercising statutory right under the UK GDPR (UK GDPR, 2018). Disclosure should not be interpreted merely as the transmission of documents. Rather, it encompasses an integrated governance process designed to balance two competing objectives i.e. protecting the individual's right of access, and protecting the rights and freedoms of third parties whose information may also appear within the requested records (Information Commissioner's Office, 2022).

Accordingly, disclosure requires organisations to distinguish between information that should be disclosed, information requiring redaction and information lawfully exempt from disclosure under the Data Protection Act 2018 (Data Protection Act, 2018). Artificial Intelligence increasingly supports each stage of this disclosure lifecycle through intelligent document identification, duplicate detection, contextual analysis and automated redaction. Nevertheless, legal accountability remains with the data controller rather than the technology itself (Ashley, 2017).

This study conceptualised data disclosure an act of revealing, transferring, granting access to, or making personal data visible to a recipient, whether that recipient is a data subject, a third-party organisation, a regulator, or the general public. In data protection law, disclosure is not limited to handing over a file; it includes any instance where data is **shared, transmitted, viewed, or otherwise made accessible** outside the original processing environment.

Data Protection

Data protection refers to the legal, technical and organisational measures designed to safeguard personal information while ensuring that individuals retain meaningful control over how their information is collected, processed and shared. The UK GDPR establishes seven foundational principles governing all processing activities that includes: Lawfulness, fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality and Accountability (UK GDPR, 2018, Art. 5).

These principles provide the legal foundation upon which Subject Access Request administration is built. AI-assisted disclosure must therefore satisfy each principle, particularly accountability, transparency and accuracy. The deployment of AI does not diminish organisational responsibility; instead, it heightens the need for demonstrable governance and oversight (Information Commissioner's Office, 2020).

Therefore, data protection is defined by this study as a set of legal, organisational, and technical measures designed to safeguard individuals' fundamental rights and freedoms concerning the processing of their personal data. The conceptual challenge for organisations is to navigate this evolving landscape with a clear understanding of their obligations, a disciplined approach to documentation and engagement, and a commitment to meaningful transparency that goes beyond regulatory minimums. The future of DSARs is not simply about data disclosure it is about making the logic of AI systems intelligible and accountable to those they affect.

Theoretical Framework

Regulatory Governance Theory (RGT)

Regulatory Governance Theory marks a shift from top-down state control to a multi-actor process of societal steering, emerging in three phases. Firstly, in the 1970s, Public Choice scholars like Stigler challenged the "public interest" view, showing regulation is often "captured" by industries for private benefit (Stigler, 1971). Secondly, the focus widened from state agencies to the broader "regulatory space," merging governance concepts (markets, networks, dialogue) with regulation. Scholars introduced the "regulatory state," where government steers society through rules rather than direct service provision. Thirdly, hybrid models like Ayres and Braithwaite's "Responsive Regulation" emerged, advocating flexible enforcement via an "enforcement pyramid" that prioritizes persuasion but escalates to punishment when needed, while involving non-state actors in "regulated self-regulation" (Ayres & Braithwaite, 1992).

Therefore, Regulatory Governance Theory (RGT), could be integrated into Artificial Intelligence (AI) hemisphere in order to examines how legal institutions regulate emerging technologies while balancing innovation against the protection of fundamental rights. Regulatory Governance Theory recognises that technological innovation frequently evolves more rapidly than legislation. Regulators must therefore develop adaptive governance mechanisms capable of encouraging innovation while protecting public interests (Black, 2008). Artificial Intelligence presents precisely this regulatory challenge. Although AI offers significant opportunities for improving Subject Access Request administration, its deployment simultaneously introduces risks concerning: (i). Algorithmic Bias; (ii). Discriminatory Outcomes; (ii) Inaccurate Document Classification; (iv) Excessive Automation; (v) opacity ("black-box" decision-making); (vi) Cybersecurity Vulnerabilities; and (vii) Erosion of Public

trust. Rather than prohibiting AI, modern regulatory approaches increasingly favour risk-based governance, whereby regulatory obligations are proportionate to the level of risk posed by the technology.

This philosophy is reflected across contemporary international governance frameworks, includes: the UK Information Commissioner's Office guidance on Artificial Intelligence (Information Commissioner's Office, 2020); the OECD Artificial Intelligence Principles (2019); the NIST Artificial Intelligence Risk Management Framework (2023); ISO/IEC 42001 Artificial Intelligence Management Systems (2023), and the European Union Artificial Intelligence Act (2024).

These frameworks consistently emphasise several common principles:

- i. transparency
- ii. explainability
- iii. fairness
- iv. human oversight
- v. accountability
- vi. proportionality
- vii. continuous risk assessment

Within the context of Subject Access Requests, Regulatory Governance Theory suggests that AI should not be evaluated solely according to technical performance but rather according to its capacity to preserve the procedural safeguards embedded within data protection legislation. This study therefore argues that future disclosure regulation should evolve from technology-neutral compliance towards AI-specific governance, ensuring that organisations deploying intelligent disclosure systems remain capable of demonstrating lawful, fair and transparent processing throughout the disclosure lifecycle.

Integration of the Theoretical Framework

Regulatory Governance Theory explains how legislators and regulators should respond to rapidly evolving AI capabilities by developing adaptive governance frameworks that protect data subjects without inhibiting technological innovation. Collectively, these theories provide an integrated analytical framework through which the legal, organisational and technological implications of AI-assisted Subject Access Requests may be critically examined. The framework further supports the article's central proposition that Artificial Intelligence should augment human legal judgement rather than replace it. While AI possesses significant capability to automate document identification, classification and preliminary review, ultimate responsibility for disclosure decisions must remain with accountable human decision-makers acting within clearly defined legal and ethical governance structures.

Methodology

This study employs a doctrinal legal research methodology combined with comparative regulatory analysis to critically examine the transformative impact of Artificial Intelligence on Subject Access Request administration under the UK GDPR. The research adopts a qualitative, non-empirical approach focused on the systematic analysis. The study analyses UK legislation including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and related statutory instruments. Regulatory guidance documents published by the Information Commissioner's Office (ICO) constitute a central source, particularly those addressing Artificial Intelligence, automated decision-making and data protection compliance. Secondary Sources: Peer-reviewed academic literature, legal scholarship, practitioner guidance and international policy documents are examined to contextualise the legal analysis.

Comparative analysis of international frameworks including the EU AI Act, OECD AI Principles, NIST AI Risk Management Framework and ISO/IEC 42001 support the identification of emerging governance standards. Analytical Framework: Regulatory Governance Theory provides the theoretical lens through which legal obligations, regulatory expectations and technological capabilities are critically evaluated. Thematic analysis identifies recurring legal, ethical and operational challenges arising from AI-assisted disclosure. Framework Development: The study synthesises legal requirements, regulatory guidance and governance principles to develop the AI-Augmented Disclosure Governance Framework (AIADGF). This framework integrates doctrinal findings, comparative insights and theoretical principles into a structured governance model for responsible AI deployment in Subject Access Request administration. The methodology emphasises interpretative rigour, doctrinal accuracy and systematic engagement with authoritative legal sources while acknowledging the rapidly evolving technological and regulatory landscape.

Reliability and Validity

Although qualitative doctrinal research does not employ statistical reliability measures, methodological rigour remains essential.

Reliability: was strengthened by relying upon authoritative legal sources capable of independent verification.

Validity: was enhanced through triangulation, whereby conclusions were supported using multiple categories of evidence, including legislation, judicial authorities, ICO guidance, international standards and peer-reviewed academic literature. Furthermore, all legal propositions presented within this study are grounded in current legislation or recognised regulatory guidance, thereby reducing interpretative bias and enhancing the credibility of the analysis.

Ethical Considerations

This study did not involve human participants, interviews, questionnaires or personal data processing. Consequently, formal institutional ethical approval was not required. Nevertheless, the research adhered to recognised principles of academic integrity by ensuring:

- i. accurate representation of legal authorities;
- ii. appropriate attribution through in-text citation;
- iii. reliance upon publicly available sources;
- iv. objective legal analysis;
- v. avoidance of plagiarism; and
- vi. balanced evaluation of competing academic perspectives.

Artificial Intelligence Technologies Transforming Subject Access Requests

The rapid advancement of Artificial Intelligence (AI) has fundamentally altered how organisations discover, retrieve, review, classify and disclose personal information. Traditional Subject Access Request (SAR) administration relied heavily upon manual document review conducted by legal professionals, compliance officers and information governance specialists. Although this approach ensured human judgement, it became increasingly unsustainable as organisations accumulated exponentially growing volumes of electronically stored information (ESI). Modern AI technologies are reshaping disclosure by introducing intelligent automation capable of processing millions of records within significantly shorter timescales while improving consistency and reducing operational costs. Nevertheless, these technologies should be regarded as decision-support tools rather than autonomous legal decision-makers.

Findings and Discussion

This study examined the legal, regulatory and operational implications of Artificial Intelligence (AI) in the administration of Subject Access Requests (SARs) under the UK General Data Protection Regulation (UK GDPR). Through doctrinal legal analysis, comparative legal research and documentary review, several significant findings emerged. The first and most significant finding is that Artificial Intelligence is fundamentally reshaping the administration of Subject Access Requests. Traditional disclosure processes were designed for environments characterised by relatively limited quantities of paper-based records. Contemporary organisations, however, manage vast repositories of electronically stored information, including emails, cloud storage, instant messaging platforms, CCTV recordings, human resource systems, customer relationship management databases and collaborative digital workspaces. The exponential growth of digital information has rendered purely manual disclosure increasingly impractical. AI technologies—including Large Language Models (LLMs), Natural Language Processing (NLP), Optical Character Recognition (OCR), semantic search and machine learning—now enable organisations to locate, classify and review documents at a speed and scale that would be impossible through conventional methods.

The research demonstrates that AI has evolved beyond a supplementary administrative tool to become a strategic component of modern information governance. Organisations are progressively integrating AI-assisted technologies into disclosure workflows to improve efficiency, reduce response times and enhance consistency. Nevertheless, technological capability alone does not ensure lawful compliance. The findings indicate that AI improves operational efficiency but does not diminish the legal obligations imposed upon data controllers. A second important finding is that the UK GDPR and the Data Protection Act 2018 remain sufficiently flexible to regulate AI-assisted disclosure despite being enacted before the widespread adoption of generative Artificial Intelligence. Rather than regulating individual technologies, UK data protection legislation adopts a principles-based approach centred upon: lawfulness; fairness; transparency; accountability; proportionality; purpose limitation; and integrity and confidentiality. These principles apply equally whether Subject Access Requests are processed manually or through AI-assisted systems. The study found no legislative gap requiring an entirely new legal framework governing AI-assisted Subject Access Requests. Instead, current legislation provides a robust legal foundation capable of accommodating technological innovation provided organisations implement appropriate governance mechanisms. This finding supports the position adopted by the Information Commissioner's Office (ICO), which consistently emphasises that existing legal obligations remain fully applicable to Artificial Intelligence (Information Commissioner's Office, 2020).

Human Oversight Remains Legally Indispensable

One of the clearest findings emerging from the research concerns the continuing importance of human judgement. Although, Artificial Intelligence demonstrates remarkable capabilities in identifying documents, recognising entities and recommending redactions, it lacks the contextual legal reasoning necessary to determine whether statutory exemptions apply under the Data Protection Act 2018.

Disclosure decisions frequently require consideration of:

- i. legal professional privilege
- ii. confidential references
- iii. national security exemptions
- iv. crime prevention exemptions
- v. management forecasting
- vi. commercial confidentiality
- vii. competing rights of third parties

These determinations involve legal interpretation rather than computational pattern recognition. Accordingly, the research demonstrates that AI should augment not replace professional disclosure officers. Meaningful human oversight remains essential to satisfy Articles 5, 22 and 24 UK GDPR while ensuring compliance with ICO guidance (Information Commissioner's Office, 2020).

Explainability is Emerging as a Core Governance Requirement

The study identifies explainability as one of the defining governance challenges associated with AI-assisted disclosure. Unlike traditional software operating through deterministic rules, many contemporary AI systems generate outputs using complex probabilistic models. Where organisations cannot explain why AI identified particular documents, recommended specific redactions or excluded relevant information, they may struggle to demonstrate accountability under Article 5(2) UK GDPR. The findings therefore indicate that explainability is evolving from an ethical aspiration into a practical legal necessity. Organisations implementing AI within Subject Access Request administration should ensure that disclosure decisions remain auditable, transparent and capable of independent review.

Discussion

The findings of this research have significant implications for legal scholarship, regulatory policy and organisational practice. Perhaps the most important implication is that Artificial Intelligence should no longer be viewed merely as an emerging technology but as an increasingly integral component of contemporary data governance. As organisations continue generating unprecedented volumes of digital information, traditional disclosure methodologies will become progressively less sustainable. Manual review processes remain accurate but are often resource-intensive, time-consuming and susceptible to inconsistency arising from reviewer fatigue. Artificial Intelligence addresses many of these operational limitations by enabling intelligent searching, automated classification and prioritisation of responsive information. Consequently, AI offers considerable potential to improve organisational compliance with statutory response deadlines under Article 12 UK GDPR.

However, efficiency should not be confused with legality. One recurring theme throughout this study is that legal compliance depends not upon the sophistication of technology but upon the quality of governance surrounding its deployment. This distinction is particularly important because increasing reliance upon AI may create an illusion of objectivity. Machine learning systems often appear impartial because they process information computationally. In reality, AI systems reflect the quality of their underlying training data, algorithmic architecture and governance arrangements. Poorly governed AI may perpetuate existing organisational biases, overlook relevant documents or generate inaccurate recommendations. Accordingly, AI introduces new governance responsibilities rather than eliminating existing legal obligations. The findings further demonstrate that Article 15 UK GDPR should be interpreted dynamically within the context of technological evolution. The statutory right of access was originally conceived within an era dominated by paper records. Today's disclosure environments involve cloud computing, distributed databases, encrypted messaging applications, collaborative platforms and increasingly sophisticated Artificial Intelligence.

Although, the technological landscape has transformed dramatically, the underlying purpose of Article 15 remains unchanged: ensuring transparency between organisations and individuals regarding the processing of personal data. Artificial Intelligence therefore represents a mechanism through which the objectives of Article 15 may be achieved more effectively rather than a justification for weakening legal safeguards. The comparative analysis undertaken within this study also reveals an important regulatory trend. While the European Union has adopted a comprehensive AI-specific legislative framework through the AI Act (European

Union, 2024), the United Kingdom continues to favour principles-based regulation supported by sector-specific guidance issued by regulators such as the ICO (Information Commissioner's Office, 2020).

Neither approach appears inherently superior. The European model provides greater legal certainty but may impose higher compliance costs and reduce regulatory flexibility. Conversely, the UK model encourages innovation but places greater responsibility upon organisations to interpret broad legal principles appropriately. The research suggests that future regulatory development may involve combining the strengths of both approaches through flexible legislation supported by detailed regulatory guidance and internationally recognised technical standards. Another significant implication concerns professional practice. Historically, Subject Access Requests have been regarded primarily as administrative compliance exercises undertaken by information governance teams. The increasing deployment of Artificial Intelligence fundamentally alters this perception. Successful AI-assisted disclosure requires interdisciplinary collaboration involving:

- i. legal professionals
- ii. data protection officers
- iii. AI engineers
- iv. cybersecurity specialists
- v. information governance practitioners
- vi. records managers
- vii. organisational leadership.

This multidisciplinary approach reflects the reality that AI governance extends beyond legal compliance into broader issues of organisational risk management, ethics and corporate accountability.

Finally, the study identifies an important gap within existing academic literature. While substantial scholarship exists concerning Artificial Intelligence generally, relatively limited research has examined its specific implications for Subject Access Request administration. By integrating doctrinal legal analysis, comparative regulatory research and governance theory, this study contributes to the emerging field of AI-enabled disclosure governance. Most significantly, it establishes the conceptual foundation for the AI-Augmented Disclosure Governance Framework (AIADGF) developed in the next section. The framework synthesises legal obligations, regulatory guidance and international best practice into a structured governance model that enables organisations to deploy Artificial Intelligence responsibly while preserving transparency, accountability and meaningful human oversight. It is intended to provide both a theoretical contribution to data protection scholarship and a practical implementation model for organisations navigating the future of AI-enabled Subject Access Requests.

Conclusion

This study has critically examined the transformative impact of Artificial Intelligence (AI) on the administration of Subject Access Requests (SARs) under the United Kingdom General Data Protection Regulation (UK GDPR). It has argued that the rapid expansion of digital information, the increasing complexity of electronically stored information, and the emergence of sophisticated AI technologies have fundamentally altered the operational environment within which organisations discharge their statutory disclosure obligations. Traditional manual approaches to SAR administration, while legally robust, are becoming progressively less capable of responding to the scale, speed and complexity of contemporary data processing. Artificial Intelligence therefore represents not merely a technological enhancement but an operational necessity for organisations seeking to maintain effective compliance with modern data protection requirements.

The research demonstrates that existing UK data protection legislation including the UK GDPR and the Data Protection Act 2018 remains sufficiently adaptable to regulate AI-assisted disclosure without the immediate need for wholly new legislation. Rather than prescribing technology-specific rules, the UK's principles-based regulatory framework requires organisations to ensure that AI-assisted processing complies with established principles of lawfulness, fairness, transparency, accountability, accuracy, integrity and proportionality. This technology-neutral approach has enabled existing legal obligations to remain relevant despite significant advances in machine learning, natural language processing, semantic search and generative AI.

However, the study also establishes that technological capability does not diminish legal responsibility. Artificial Intelligence may dramatically improve document retrieval, information classification, automated redaction and workflow management, but responsibility for lawful disclosure remains firmly with the data controller. Organisations cannot delegate statutory accountability to algorithms, software vendors or automated systems. Every disclosure decision must remain capable of human explanation, legal justification and regulatory scrutiny. In this respect, the accountability principle contained within Article 5(2) UK GDPR continues to provide the cornerstone of lawful AI deployment.

One of the central findings of this research is that meaningful human oversight remains indispensable. Although AI systems increasingly demonstrate remarkable capabilities in identifying relevant documents and recognising complex data patterns, they cannot presently replicate the contextual legal reasoning required when interpreting statutory exemptions, balancing competing rights or assessing proportionality. Decisions involving legal professional privilege, confidential references, national security, management forecasting or the rights of third parties require nuanced legal judgement that extends beyond computational prediction. Consequently, AI should be viewed as an augmentation of professional expertise rather than a replacement for qualified disclosure practitioners.

The study further identifies explainability as one of the defining challenges of AI governance within Subject Access Request administration. As AI models become increasingly sophisticated, organisations must ensure that disclosure decisions remain transparent, auditable and capable of meaningful explanation. Explainability is no longer merely an ethical aspiration but an operational requirement underpinning legal accountability. Without transparent governance arrangements, organisations may struggle to demonstrate compliance with Articles 5, 12, 15, 22, 24, 25 and 35 UK GDPR or satisfy the expectations articulated by the Information Commissioner's Office (ICO).

Comparative analysis undertaken in this research reveals growing international convergence around several fundamental principles of AI governance. Despite differences in legislative architecture between the United Kingdom, the European Union, the United States, Canada and Australia, common themes consistently emerge, including transparency, accountability, fairness, privacy by design, human oversight and risk management. This convergence suggests that future AI regulation is likely to evolve through the harmonisation of governance principles supported by internationally recognised standards rather than through complete legislative uniformity. The increasing influence of the OECD Artificial Intelligence Principles, the NIST Artificial Intelligence Risk Management Framework, ISO/IEC 42001 and the European Union AI Act illustrate this trend towards globally recognised governance norms.

The principal scholarly contribution of this article is the development of the **AI-Augmented Disclosure Governance Framework (AIADGF)**. Unlike existing disclosure models that concentrate primarily on procedural compliance, the AIADGF integrates legal obligations, organisational governance and AI-enabled technologies into a structured eight-stage governance model. The framework positions Artificial Intelligence as an intelligent decision-support mechanism operating within an environment characterised by meaningful human

oversight, explainability, auditability and continuous organisational learning. By embedding accountability throughout the disclosure lifecycle—from request validation and intelligent data discovery to legal review, quality assurance and post-disclosure evaluation—the framework provides a practical roadmap for organisations seeking to modernise Subject Access Request administration without compromising fundamental rights.

The AIADGF therefore contributes both theoretically and practically to the emerging field of AI governance. Theoretically, it advances legal scholarship by proposing an integrated governance model specifically designed for AI-assisted disclosure under the UK GDPR. Practically, it offers organisations a structured implementation framework capable of enhancing compliance, improving operational efficiency and strengthening public trust in AI-enabled information governance. The framework also provides regulators with a conceptual basis upon which future guidance concerning AI-assisted Subject Access Requests may be developed. The research acknowledges several limitations. Given the rapid pace of technological innovation, AI capabilities continue to evolve faster than legislative and regulatory responses. Consequently, certain governance challenges identified in this study may require further examination as emerging technologies including multimodal AI, autonomous agents and advanced privacy-enhancing technologies become increasingly integrated into organisational information systems. Future empirical research examining organisational implementation of AI-assisted Subject Access Request systems, user confidence, regulatory investigations and judicial interpretation will further enrich understanding of this evolving area. Notwithstanding these limitations, the findings demonstrate that the future of Subject Access Request administration will not be characterised by fully autonomous disclosure systems. Instead, the evidence supports the emergence of an **AI-augmented disclosure environment** in which Artificial Intelligence enhances efficiency while accountable human decision-makers retain ultimate responsibility for legality, fairness and transparency. Organisations that successfully integrate technological innovation with robust governance structures will be better positioned to satisfy both regulatory expectations and public confidence in an increasingly data-driven society. Ultimately, Artificial Intelligence should not be regarded as replacing the principles upon which data protection law is founded. Rather, it should serve as a powerful instrument for strengthening those principles by improving access, consistency, accountability and procedural fairness. The enduring objective of Article 15 UK GDPR to empower individuals through transparency—remains unchanged. What is changing is the technological means through which that objective can be achieved. The challenge for policymakers, regulators and organisations is therefore not whether Artificial Intelligence should be used in Subject Access Request administration, but how it can be governed responsibly so that innovation reinforces, rather than undermines, the fundamental rights that lie at the heart of the UK's data protection regime.

Recommendations

Drawing upon the findings of this research, the following recommendations are proposed for policymakers, regulators, organisations and researchers.

i. **Government and Policymakers:** The UK Government should develop sector-specific guidance addressing the use of Artificial Intelligence in Subject Access Request administration while preserving the flexibility of the UK's principles-based data protection regime. Future legislative reforms should clarify governance expectations for AI-assisted disclosure without creating unnecessary barriers to responsible innovation.

ii. **Information Commissioner's Office:** The ICO should publish dedicated guidance on AI-assisted Subject Access Requests, including practical expectations concerning explainability, human oversight, algorithm validation, automated redaction, audit trails and

governance documentation. Such guidance would provide organisations with greater regulatory certainty and promote consistent implementation across sectors.

iii. **Organisations:** Organisations should adopt formal AI governance frameworks before deploying AI within Subject Access Request processes. This includes conducting Data Protection Impact Assessments (DPIAs), establishing multidisciplinary governance teams, maintaining comprehensive audit logs, validating AI outputs through meaningful human review and implementing continuous performance monitoring. AI should support—not replace—professional legal judgement.

iv. **Technology Developers:** Developers of AI-assisted disclosure platforms should prioritise transparency, explainability, security and interoperability. Systems should be capable of producing verifiable audit trails, confidence scores and explainable outputs to facilitate regulatory compliance and independent review.

v. **Professional Training:** Data Protection Officers, legal practitioners, information governance professionals and AI specialists should receive interdisciplinary training combining data protection law, AI governance, ethics and information management. Future compliance will increasingly depend upon professionals capable of bridging legal and technological expertise.

vi. **International Cooperation:** Given the global nature of data processing, international cooperation between regulators should be strengthened through greater alignment of AI governance principles, technical standards and regulatory guidance. Continued collaboration between the ICO, the European Data Protection Board, OECD, ISO, NIST and other international bodies will promote greater consistency while supporting responsible cross-border innovation.

vii. **Future Research:** Future research should move beyond doctrinal analysis to include empirical studies examining organisational implementation of AI-assisted Subject Access Request systems, user confidence, regulatory enforcement trends and comparative judicial interpretation. Longitudinal studies evaluating the effectiveness of governance frameworks such as the AI-Augmented Disclosure Governance Framework (AIADGF) would further strengthen the evidence base for responsible AI deployment within data protection practice.

References

- Alon, U., Kamfonas, M. and Gonen, H. (2024) *How Large Language Models Reason*. arXiv preprint.
- Alston, P. (2022). *Digital governance and human rights*. Oxford University Press.
- Armstrong, J., & Ford, S. (2023). AI-assisted disclosure in data protection compliance. *Journal of Data Protection Law*, 15(2), 112–134.
- Article 29 Working Party (2017) *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation (EU) 2016/679*. Brussels: European Commission.
- Ashley, K. D. (2017). *Artificial intelligence and legal analytics: New tools for law practice in the digital age*. Cambridge University Press.
- Ashley, K. D. (2017). *Artificial intelligence and legal analytics: New tools for law practice in the digital age*. Cambridge University Press.
- Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press.
- Barocas, S., Hardt, M., & Narayanan, A. (2019). *Fairness and machine learning*. MIT Press.
- Bennett, C. J., & Raab, C. D. (2021). *The governance of privacy: Policy instruments in global perspective* (2nd ed.). MIT Press.
- Bennett, C.J. (2018) *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd edn. Cambridge, MA: MIT Press.
- Binns, R. (2020). On the apparent conflict between individual and group fairness. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 514–524.
- Black, J. (2008) ‘Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes’, *Regulation & Governance*, 2(2), pp. 137–164.
- Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Regulation & Governance*, 2(2), 137-164.
- Bommasani, R. et al. (2021) *On the Opportunities and Risks of Foundation Models*. Stanford University, Center for Research on Foundation Models.
- Bowen, G.A. (2009) ‘Document Analysis as a Qualitative Research Method’, *Qualitative Research Journal*, 9(2), pp. 27–40.
- Buchanan, J. (2024). Automation and accountability in data subject access. *International Data Privacy Law*, 14(1), 45–62.
- Bygrave, L.A. (2022) *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press.
- Cabrera, M., & Walker, T. (2022). E-disclosure and AI in financial services regulation. *Journal of Financial Regulation*, 8(3), 201–225.
- Carey, P. (2024) *Data Protection: A Practical Guide to UK and EU Law*. 7th edn. Oxford: Oxford University Press.
- Council of Europe (1981) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)*.
- Creswell, J.W. and Creswell, J.D. (2023) *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. 6th edn. Thousand Oaks, CA: Sage.
- Crootof, R. (2021). Cyborg justice. *Washington University Law Review*, 98(5), 1245–1310.
- Dale, R. (2021). Natural language processing in legal technology. *Natural Language Engineering*, 27(4), 509–524.
- Data Protection Act 2018, c. 12.
- Data Protection Act 2018, c. 12. <https://www.legislation.gov.uk/ukpga/2018/12/contents>
- Data Protection Act 2018, c. 12. <https://www.legislation.gov.uk/ukpga/2018/12/contents>
- Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74.

- Department for Science, Innovation and Technology (2023) *A Pro-Innovation Approach to AI Regulation*. London: HMSO.
- Department for Science, Innovation and Technology (2024) *Responsible AI in the UK*. London: HMSO.
- Durant v Financial Services Authority [2003] EWCA Civ 1746.
- Edwards, L., & Veale, M. (2021). Accountability and data protection in AI systems. *European Data Protection Law Review*, 7(2), 191–205.
- European Commission (2020) *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*. Brussels.
- European Commission (2024) *Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. Brussels.
- European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence*. European Union.
- European Data Protection Board (2020) *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*.
- European Data Protection Board (2022) *Guidelines on Data Subject Rights – Right of Access*.
- European Parliament. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act)*. Official Journal of the European Union.
- European Union (2016) *Regulation (EU) 2016/679 (General Data Protection Regulation)*.
- European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
- Floridi, L. (2014) *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press.
- Floridi, L. (2023) *The Ethics of Artificial Intelligence*. Oxford: Oxford University Press.
- Goodfellow, I., Bengio, Y. and Courville, A. (2016) *Deep Learning*. Cambridge, MA: MIT Press.
- Grossman, M.R. and Cormack, G.V. (2011) ‘Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient than Exhaustive Manual Review’, *Richmond Journal of Law and Technology*, 17(3), pp. 1–48.
- Harrington, S. (2023). Healthcare data access and AI: Navigating UK GDPR compliance. *Medical Law Review*, 31(4), 589–612.
- Hildebrandt, M. (2020) *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press.
- House of Commons Science, Innovation and Technology Committee (2023) *The Governance of Artificial Intelligence*. London: HMSO.
- Hutchinson, T. and Duncan, N. (2012) ‘Defining and Describing What We Do: Doctrinal Legal Research’, *Deakin Law Review*, 17(1), pp. 83–119.
- Information Commissioner’s Office (2019) *Explaining Decisions Made with Artificial Intelligence*. Wilmslow: ICO.
- Information Commissioner’s Office (2020) *AI Auditing Framework*. Wilmslow: ICO.
- Information Commissioner’s Office (2021) *Guidance on AI and Data Protection*. Wilmslow: ICO.
- Information Commissioner’s Office (2023a) *Guide to UK GDPR*. Wilmslow: ICO.
- Information Commissioner’s Office (2023b) *Right of Access Guidance*. Wilmslow: ICO.
- Information Commissioner’s Office (2023c) *Subject Access Requests Guidance*. Wilmslow: ICO.
- Information Commissioner’s Office (2024) *Data Protection Impact Assessments Guidance*. Wilmslow: ICO.

- Information Commissioner's Office. (2020). *Explaining decisions made with AI*. ICO Guidance.
- Information Commissioner's Office. (2020). *Guidance on the AI auditing framework*. <https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-the-ai-auditing-framework-2-1.pdf>
- Information Commissioner's Office. (2020). *Guidance on the AI auditing framework*. Retrieved from <https://ico.org.uk>
- Information Commissioner's Office. (2021). *Accountability and governance framework for data protection*. ICO.
- Information Commissioner's Office. (2022). *Right of access guidance*. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/>
- Information Commissioner's Office. (2023). *Subject Access Requests: Guidance for organisations*. ICO.
- International Organization for Standardization (2023) *ISO/IEC 42001:2023 Artificial Intelligence Management Systems*. Geneva: ISO.
- International Organization for Standardization (2024) *ISO/IEC 23894: Artificial Intelligence – Risk Management*. Geneva: ISO.
- Ittihadieh v 5–11 Cheyne Gardens RTM Co Ltd [2017] EWCA Civ 121.
- Katsh, E., & Rabinovich-Einy, O. (2021). *Digital justice: Technology and the internet of disputes*. Oxford University Press.
- Kuner, C. (2020) *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press. *Lees v Lloyds Bank plc* [2022] EWHC 2249 (Ch).
- Mayer-Schönberger, V. and Cukier, K. (2013) *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.
- McGregor, L., Murray, D. and Ng, V. (2019) 'International Human Rights Law as a Framework for Algorithmic Accountability', *International & Comparative Law Quarterly*, 68(2), pp. 309–343.
- Millard, C. (2022). Cloud computing and data protection: Challenges for SARs. *Computer Law & Security Review*, 45, 105–122.
- Mittelstadt, B., Wachter, S., & Russell, C. (2023). The ethics of AI-assisted legal decision-making. *AI & Society*, 38(2), 521–538.
- Mittelstadt, B.D. et al. (2016) 'The Ethics of Algorithms', *Big Data & Society*, 3(2).
- Mudassir, N. (2025) The Impact of Artificial Intelligence (AI) In Crime Detection and Prevention in Nigeria. *African Journal of Modern Society*. ISSN: 2141-3878, Ppg. 1-16.
- National Institute of Standards and Technology (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg, MD: NIST.
- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. NIST.
- OECD. (2019). *Recommendation of the Council on Artificial Intelligence*. OECD Publishing.
- Organisation for Economic Co-operation and Development (2019) *OECD Principles on Artificial Intelligence*. Paris: OECD.
- Organisation for Economic Co-operation and Development (2023) *OECD AI Policy Observatory*. Paris: OECD.
- Pasquale, F., & Cashwell, J. (2022). AI and the rule of law: Augmentation not replacement. *Harvard Journal of Law & Technology*, 35(1), 101–148.
- Pearce, F. (2022) *Artificial Intelligence and Data Protection Law*. London: Sweet & Maxwell.
- Purtova, N. (2018) 'The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law', *Law, Innovation and Technology*, 10(1), pp. 40–81.

- Russell, S. and Norvig, P. (2021) *Artificial Intelligence: A Modern Approach*. 4th edn. Harlow: Pearson.
- Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Sartor, G. and Lagioia, F. (2020) 'The Impact of the General Data Protection Regulation on Artificial Intelligence', *European Journal of Risk Regulation*, 11(4), pp. 717–746.
- Scherer, M. U. (2023). Regulating AI in data protection contexts. *Columbia Law Review*, 123(4), 1127–1180.
- Selbst, A.D. et al. (2019) 'Fairness and Abstraction in Sociotechnical Systems', *Proceedings of FAT 2019*, pp. 59–68.
- Solove, D.J. and Schwartz, P.M. (2024) *Information Privacy Law*. 8th edn. New York: Aspen.
- Surden, H. (2019). Artificial intelligence and law: An overview. *Georgia State University Law Review*, 35(4), 1301–1337.
- Susskind, R. (2019) *Online Courts and the Future of Justice*. Oxford: Oxford University Press.
- Susskind, R. (2022). *Tomorrow's lawyers: An introduction to your future* (3rd ed.). Oxford University Press.
- Susskind, R. (2023) *How to Think About AI*. Oxford: Oxford University Press.
- The Alan Turing Institute (2021) *Understanding Artificial Intelligence Ethics and Safety*. London.
- UK General Data Protection Regulation (UK GDPR). (2018). <https://www.legislation.gov.uk/eur/2016/679/contents>
- UK General Data Protection Regulation. (2018). <https://www.legislation.gov.uk/eur/2016/679>
- United Kingdom (2018a) *Data Protection Act 2018*. London: HMSO.
- United Kingdom (2018b) *European Union (Withdrawal) Act 2018*. London: HMSO.
- United Kingdom (2019) *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019*. London: HMSO.
- United Kingdom (2021) *National AI Strategy*. London: HMSO.
- United Kingdom (2023) *AI Regulation White Paper*. London: HMSO.
- United Kingdom (2025) *Data (Use and Access) Act 2025*. London: HMSO.
- United Kingdom Government (2023) *Generative AI Framework for HM Government*. London: HMSO.
- United Kingdom Government (2024) *Algorithmic Transparency Recording Standard*. London: HMSO.
- United Kingdom Parliament (2023) *House of Lords Communications and Digital Committee: Large Language Models and Generative AI*. London: HMSO.
- United Kingdom Parliament (2024) *Artificial Intelligence (Regulation) Bill [HL]*. London: HMSO.
- United Kingdom Parliament (2025) *Data (Use and Access) Act Explanatory Notes*. London: HMSO.
- United Nations Educational, Scientific and Cultural Organization (2021) *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO.
- Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 30, 5998–6008.
- Veale, M. and Edwards, L. (2018) 'Clarity, Surprises and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling', *Computer Law & Security Review*, 34(2), pp. 398–404.
- Veale, M., & Zuiderveen Borgesius, F. J. (2021). Demystifying the draft EU AI Act. *Computer Law Review International*, 22(4), 97–112.

- Veale, M., Van Kleek, M. and Binns, R. (2018) 'Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making', *Proceedings of CHI 2018*.
- Wachter, S., Mittelstadt, B. and 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), pp. 76–99.
- Wachter, S., Mittelstadt, B. and Russell, C. (2021) 'Bias Preservation in Machine Learning', *Nature Machine Intelligence*, 3(3), pp. 1–8.
- Wachter, S., Mittelstadt, B., & Russell, C. (2024). Hallucinations and accountability in LLMs. *Nature Machine Intelligence*, 6(1), 34–45.
- West, S.M., Whittaker, M. and Crawford, K. (2019) *Discriminating Systems: Gender, Race and Power in AI*. AI Now Institute.
- Wolford, K. (2020). *Understanding the GDPR: A practical guide*. Privacy International.
- Yeung, K. (2023). Algorithmic regulation and governance. *Oxford Journal of Legal Studies*, 43(1), 88–115.
- Zarsky, T. (2016) *Incompatible: The GDPR in the Age of Big Data*. Oxford: Oxford University Press.
- Zhou, J., Liu, Y., & Chen, X. (2023). Large language models for legal document processing. *IEEE Transactions on Knowledge and Data Engineering*, 35(8), 7890–7905.
- Zuboff, S. (2019) *The Age of Surveillance Capitalism*. London: Profile Books.