Artificial Intelligence, GDPR Compliance, and Automated Decision-Making: A Doctrinal Analysis of Legal Accountability and Data Protection Risks in the UK and EU

ABSTRACT

Artificial intelligence (AI) systems increasingly shape decisions about employment, credit scoring, healthcare prioritisation, immigration screening, security, and public services. Such developments introduce significant data-protection risks, particularly where automated decision-making (ADM) processes are opaque, large-scale, and potentially discriminatory. This dissertation examines whether the General Data Protection Regulation (GDPR), UK GDPR, and supporting regulatory guidance provide a sufficiently robust framework to govern modern AI-driven ADM systems.

Using a doctrinal legal research methodology, the study analyses legislation, case law, regulatory decisions, academic commentary, and policy documents. The findings indicate that while GDPR principles — fairness, transparency, accountability, data minimisation, and purpose limitation — remain highly relevant, the practical enforcement of these principles is strained by the technical opacity of machine-learning models. Ambiguities surrounding Article 22 on automated decision-making, divergent interpretations by supervisory authorities, and limited guidance on algorithmic explainability contribute to inconsistent compliance across sectors.

The dissertation concludes that a harmonised, risk-based model of AI governance is needed: one that combines GDPR's rights-based approach with the structured obligations introduced by the EU AI Act and the UK's pro-innovation regulatory strategy. Strengthening supervisory guidance, embedding mandatory algorithmic audits, and clarifying accountability for developers and deployers are essential steps toward ensuring lawful, transparent, and rights-respecting AI systems.

CHAPTER 1: INTRODUCTION

1.1 Background

The adoption of artificial intelligence (AI) and automated decision-making (ADM) has accelerated across both public and private sectors. Banks rely on predictive models to evaluate loan eligibility. Employers use machine-learning classifiers to shortlist job applicants. Public authorities apply ADM tools to assess welfare eligibility, detect fraud, and analyse risk scores. Healthcare providers use clinical algorithms to support diagnostics and resource allocation.

These developments offer clear efficiency gains but pose equally significant risks. Unlike traditional rule-based systems, modern AI models operate through complex, data-driven statistical correlations, often producing outcomes that are difficult — or impossible — to fully interpret. Such opacity challenges the core data-protection values embedded in the GDPR and UK GDPR, including transparency, fairness, accountability, and the right to meaningful human oversight.

1.2 Research Problem

While the GDPR establishes comprehensive rules for the processing of personal data, questions remain about its practical effectiveness when applied to sophisticated AI models. Organisations frequently struggle to:

- explain AI-generated outcomes in a legally meaningful way;
- identify valid lawful bases for large-scale training data;
- demonstrate proportionality and fairness in automated profiling;
- manage the risks of bias, discrimination, and inaccurate outputs;
- maintain clear accountability between AI developers and deployers.

Regulators themselves acknowledge gaps. Supervisory authorities have published guidance, but interpretations differ between the ICO, CNIL, AEPD, and other EU bodies. This inconsistency complicates compliance for organisations operating across multiple jurisdictions.

1.3 Aim of the Study

The aim of this dissertation is to evaluate whether current data-protection law — primarily the GDPR, UK GDPR, and related regulatory guidance — provides a sufficiently clear and enforceable framework for governing AI-driven ADM systems.

1.4 Research Objectives

1. To analyse the legal obligations that apply to AI-driven automated decision-making under the GDPR and UK GDPR.
2. To evaluate the adequacy and limitations of Article 22 and related transparency requirements.
3. To examine relevant case law and regulatory enforcement trends.

4. To compare existing data-protection frameworks with emerging AI-specific regulations such as the EU AI Act.
5. To identify gaps and propose legally grounded recommendations for improved AI governance.

1.5 Significance of the Study

This research contributes to ongoing academic and policy debates by offering a structured, doctrinal legal analysis of AI governance. It provides clarity for researchers, regulators, and organisations seeking to deploy AI technologies responsibly. The findings demonstrate how established legal principles can be applied to new technological contexts while highlighting areas where interpretation and enforcement require further development.

1.6 Structure of the Dissertation

- **Chapter 1** introduces the research topic and objectives.
- **Chapter 2** reviews academic and regulatory literature relating to AI and data protection.
- **Chapter 3** outlines the doctrinal methodology and sources.
- **Chapter 4** analyses key legal provisions, case law, and regulatory decisions.
- **Chapter 5** discusses the implications of these findings.
- **Chapter 6** offers conclusions and recommendations.

CHAPTER 2: LITERATURE REVIEW (EXCERPT)

(The following is an extract — the full chapter is available on request.)

2.1 The Evolution of Data-Protection Law in the Digital Age

European data-protection law is rooted in principles of autonomy, dignity, and informational self-determination. The GDPR strengthened these foundations by introducing accountability, enhanced transparency obligations, and stronger enforcement powers. However, scholars argue that the regulation was drafted before the rise of deep learning, and therefore its general principles now require technologically informed interpretation.

2.2 Automated Decision-Making and Profiling

Academic literature distinguishes between:

- **profiling**, which involves automated processing to analyse or predict personal characteristics; and
- **automated decision-making**, where a decision is made solely by automated means without human involvement.

Article 22 of the GDPR provides individuals with protections against decisions that have legal or similarly significant effects. However, academics and regulators continue to debate the scope, enforceability, and practical meaning of this provision, especially in high-risk ADM contexts.

2.3 Transparency and Explainability

A central issue in AI governance is the extent to which organisations can meaningfully explain complex model behaviour. Scholars highlight tensions between:

- transparency obligations under Articles 13–15;
- trade-secret and IP protections;
- the inherent opacity of machine-learning systems.

Regulators increasingly emphasise that explanations must be “meaningful,” tailored to human understanding, and sufficient to allow individuals to challenge decisions.

2.4 Algorithmic Bias and Discrimination

The literature documents multiple instances where AI systems have produced discriminatory outcomes due to biased training data or flawed design assumptions. Examples include recruitment tools favouring certain demographics, risk-scoring systems penalising minority communities, and clinical algorithms underestimating the needs of specific patient groups.

This raises questions about how fairness should be interpreted legally and whether existing equality and data-protection frameworks are adequate.

CHAPTER 3: METHODOLOGY (EXCERPT)

This dissertation adopts a **doctrinal legal methodology**, examining:

- primary legal sources (GDPR, UK GDPR, EU AI Act),
- case law from EU courts and national supervisory authorities,
- regulatory reports from the ICO, EDPB, and CNIL,
- academic commentary and policy papers.

Doctrinal analysis is used to interpret legal texts, identify ambiguities, and examine how different authorities apply principles in practice.

To comply with ethical standards, only extracts of the dissertation are published publicly. The **full sample (120+ pages including methodology, findings, discussion, and appendices)** is available privately.