International Journal of Sustainable Development and Planning
Vol. 20, No. 6, June, 2025, pp. 2639-2650
Journal homepage: http://iieta.org/journals/ijsdp

Legal Challenges of Using AI and Big Data in Public Administration: Administrative Liability, Data Protection, and Public Services Efficiency

Hisham Hamed Al-Kasasbeh[1], Nasir Albalawee[2], Haneen A. Al-Khawaja[3*], Ali Khaled Qtaishat[4]

[1] Department of Law, Al-Zaytoonah University of Jordan, Amman 11733, Jordan
[2] Department of Law, Jadara University, Irbid 21110, Jordan
[3] Department of Financial Technology and Banking, Faculty of Business, Ajloun National University, Ajloun 26810, Jordan
[4] Private Law Department, Al-Ahliyya Amman University, Amman 19328, Jordan

Corresponding Author Email: h.alkhawaja@anu.edu.jo

https://doi.org/10.18280/ijsdp.200631

Received: 18 April 2025
Revised: 13 June 2025
Accepted: 18 June 2025
Available online: 30 June 2025

Keywords:
AI governance, administrative liability, Legal Risk Index (LRI), public sector automation, data protection compliance

ABSTRACT

This study investigates the evolving legal challenges posed by the integration of artificial intelligence and big data in public administration. Through a mixed-method approach, combining doctrinal legal analysis, case study review, and empirical dataset evaluation, it examines how current laws respond to emerging risks in administrative liability, data protection, and service automation. A novel Legal Risk Index (LRI) was developed to quantify regulatory sensitivity across jurisdictions and application domains, revealing that systems in welfare fraud detection and biometric surveillance face the highest legal scrutiny, with LRI scores reaching critical thresholds in over 70% of examined cases. The study analyzed a dataset of 140+ public sector AI deployments across Europe, offering a concrete empirical base. The paper compares AI governance strategies in the EU, UK, US, and MENA, highlighting disparities in oversight, enforcement, and public accountability. The findings show that legal maturity, not just technological advancement, is key to responsible deployment. Major contributions include the introduction of a cross-jurisdictional legal risk framework, evidence-based policy recommendations, and a structured model for liability allocation in AI-driven decisions. This research offers practical insights for regulators and public institutions seeking to balance innovation with rights-based governance.

1. INTRODUCTION

In recent years, AI and big data have emerged as transformative forces across various sectors, including public administration. Governments worldwide are leveraging these technologies to enhance decision-making processes, improve service delivery, and increase operational efficiency. AI applications, such as machine learning algorithms and predictive analytics, enable public institutions to analyse vast datasets, identify patterns, and make informed decisions. Big data facilitates the collection and processing of extensive information from diverse sources, providing valuable insights for policy formulation and implementation.

For instance, the European Union has been proactive in integrating AI into public services. The EU's AI Act aims to regulate AI applications, ensuring they are used ethically and effectively within public administration [1]. Similarly, the United Kingdom has developed guidance on AI and data protection to assist organizations in adopting AI technologies while safeguarding individuals' rights [2].

While the adoption of AI and big data offers numerous benefits, it also raises significant legal and ethical concerns. The deployment of these technologies in public administration must strike a delicate balance between fostering innovation and ensuring legal accountability. Unregulated or inadequately governed AI systems can lead to unintended consequences, such as biased decision-making, privacy infringements, and a lack of transparency [3].

The UK's Information Commissioner's Office emphasizes the necessity of embedding fairness into AI systems to comply with data protection laws and maintain public trust [2]. Similarly, the EU's AI Act underscores the importance of establishing a legal framework that mitigates risks associated with AI applications in the public sector [1].

This paper aims to address the following research questions:

What are the legal implications of using AI in public administration?

How does big data affect administrative decision-making and service delivery?

What legal frameworks govern data protection and liability in public sector AI?

This study contributes to the existing body of knowledge by providing a comprehensive analysis of the legal challenges associated with AI and big data in public administration. It examines current legal frameworks, identifies gaps, and offers recommendations for policymakers and public institutions to navigate the complexities of integrating these technologies responsibly.

The paper is structured as follows: section 2 reviews the existing literature on AI in public administration, cyber law, legal responsibility, data protection regulations, and approaches to public sector digitization. An explanation of the research methods employed, including legal doctrinal analysis, case study examination, and dataset-based analysis, is explained in section 3. In section 4, the definition and scope of administrative liability, challenges in attributing liability to AI systems, and proposals for liability distribution are discussed. Section 5 analyses legal frameworks governing data protection, risks of data breaches, ethical implications, and relevant case studies. Section 6 explores how AI and big data improve efficiency, legal tensions between automation and fairness, and the impact of accountability frameworks on service delivery. A comparison of legal approaches to AI and data use in public administration across different regions is presented in section 7. Finally, a recap of major findings, answers to the research questions, and suggestions for future research directions are concluded in section 8.

This study contributes to the existing body of knowledge by providing a comprehensive analysis of the legal challenges associated with AI and big data in public administration. It examines current legal frameworks, identifies gaps, and offers recommendations for policymakers and public institutions to navigate the complexities of integrating these technologies responsibly. Methodologically, the study adopts a three-part approach combining doctrinal legal analysis, comparative case study evaluation, and empirical dataset-based investigation to ensure both theoretical depth and practical relevance. Notably, the research introduces a novel Legal Risk Index (LRI) — a structured metric to assess legal vulnerability in AI deployment across jurisdictions and application domains, marking an original contribution to the field.

2. LITERATURE REVIEW

This section is structured to transition from a broad examination of the integration of Artificial Intelligence (AI) and big data in public administration to more specific discussions on cyber law, legal responsibilities, data protection frameworks, and approaches to public sector digitization.

The adoption of AI and big data technologies has significantly transformed public administration, enhancing efficiency, transparency, and service delivery. Governments worldwide are increasingly leveraging these technologies to process vast amounts of data, enabling informed decision-making and personalized public services. For instance, a systematic literature review highlights the growing interest in implementing AI-based software in the public sector, emphasizing the need to understand citizens' acceptance of such technologies [4]. However, this integration also introduces challenges related to ethical considerations, data privacy, and the potential for algorithmic bias. Addressing these challenges necessitates a comprehensive understanding of the legal frameworks governing AI and big data in public administration [5].

The rapid integration of AI into public administration has outpaced the development of corresponding legal frameworks, leading to complex issues concerning accountability and transparency. Traditional legal systems often struggle to attribute responsibility for decisions made or influenced by AI systems. The UK's proposed approach to AI regulation emphasizes a sectoral, risk-based framework, advocating for principles that ensure AI is used safely, is technically secure, transparent, fair, and that legal persons are clearly responsible for AI governance [6]. Despite these initiatives, the dynamic nature of AI technologies presents ongoing challenges in establishing comprehensive legal responsibilities.

Data protection remains a critical concern in the deployment of AI and big data within public administration. The European Union's General Data Protection Regulation (GDPR) sets stringent guidelines for data processing, emphasizing individual consent, transparency, and the right to privacy. In the UK, the Data Protection Act 2018 and the UK GDPR govern data protection practices, imposing obligations on organizations to ensure lawful processing of personal data [2]. The UK's Data Protection and Digital Information Bill, introduced in 2022, aims to update the existing framework to accommodate advancements in digital technologies, including AI [7]. However, the effective enforcement of these regulations in the context of AI-driven public services remains a subject of ongoing debate [8].

The digitization of public services involves the integration of digital technologies into governmental processes to enhance efficiency and accessibility. While this transformation offers significant benefits, it also raises legal and ethical considerations. The UK's "Transforming for a Digital Future" policy outlines ambitions to revolutionize digital public services, emphasizing the need for robust legal frameworks to support this transition [9]. Similarly, the Organization for Economic Co-operation and Development (OECD) provides principles to guide policymakers in designing and delivering public services fit for the digital age, highlighting the importance of legal considerations in digital governance [10]. These approaches underscore the necessity of aligning legal frameworks with technological advancements to ensure the protection of citizens' rights and the effective delivery of public services.

Despite the growing body of literature on AI and big data in public administration, several gaps remain. There is a need for more empirical studies examining the practical implications of AI deployment in public services, particularly concerning legal accountability and data protection. Additionally, research exploring the effectiveness of existing legal frameworks in addressing the unique challenges posed by AI technologies is limited. Furthermore, comparative analyses of international approaches to AI regulation in public administration could provide valuable insights into best practices and inform policy development.

Despite the growing body of literature on AI and big data in public administration, several gaps remain. There is a need for more empirical studies examining the practical implications of AI deployment in public services, particularly concerning legal accountability and data protection. Additionally, research exploring the effectiveness of existing legal frameworks in addressing the unique challenges posed by AI technologies is limited. Furthermore, comparative analyses of international approaches to AI regulation in public administration could provide valuable insights into best practices and inform policy development.

In summary, the following research gaps are identified:

- Lack of empirical data assessing legal risks in real-world AI deployments in public administration.
- Insufficient evaluation of how existing legal frameworks respond to AI-related liability and data protection issues.

- Limited comparative studies analyzing cross-jurisdictional legal responses to administrative AI use.
- Absence of structured tools (e.g., indices or scoring systems) to measure legal vulnerability in public sector AI applications.

3. METHODOLOGY

In legal-technical studies where both law and data intersect, the methodology accounts for normative legal analysis and empirical data exploration. This section begins with a general overview of our research approach and then delves into specific techniques used, including doctrinal legal research, international case studies, and data-driven analysis using publicly available datasets.

3.1 The methodological approach

This study adopts a triangulated research methodology that merges doctrinal legal analysis, comparative case study evaluation, and empirical dataset-based investigation. The goal is to construct a well-rounded understanding of the legal challenges associated with the use of AI and big data in public administration. This combination of methods is necessary due to the interdisciplinary nature of the research, which deals with both normative legal structures and real-world technological implementations.

3.1.1 Legal doctrinal method

At the core of this research lies the legal doctrinal approach, a classical methodology in legal scholarship. It involves an in-depth examination of existing legal materials such as statutes, regulatory texts, court rulings, and administrative guidelines. For this study, legal texts and regulatory documents are selected based on their direct relevance to AI and data governance in the public sector. Specific legal instruments analysed include:

i. The EU Artificial Intelligence Act, with its risk-tiered regulatory structure for AI systems in public services.
ii. The General Data Protection Regulation (GDPR) and UK GDPR, particularly provisions on automated decision-making, profiling, and consent.
iii. National administrative law provisions governing public accountability and liability.

In addition to interpreting the letter of the law, this method evaluates how legal principles such as transparency, proportionality, and fairness are applied in the context of AI-based governance. It also examines how judicial interpretations, particularly from administrative courts, have dealt with AI-induced decision-making errors or data misuse.

3.1.2 Case study analysis

To contextualize the doctrinal findings and uncover jurisdiction-specific nuances, this study integrates a comparative case study analysis. This component explores how different countries are grappling with legal and ethical challenges emerging from AI deployment in public services.

Three case studies are selected to represent a spectrum of regulatory environments:

European Union (EU): Examines how the proposed AI Act interfaces with GDPR, with examples such as digital ID systems and smart public safety projects.

United Kingdom (UK): Focuses on the implementation of AI tools for welfare fraud detection and predictive service allocation under the Data Protection Act 2018.

US (US): Highlights controversial AI applications like predictive policing and automated risk scoring in social services, assessed within a less centralized legal framework.

Each case is evaluated using a consistent framework:

The type of AI used

The nature of the public service

The regulatory instruments applied

Public and judicial response

The outcome in terms of legality, efficiency, and public trust.

This approach allows us to compare not only how laws are written, but also how they are operationalized or challenged in live administrative contexts.

3.1.3 Dataset-based analysis

To supplement doctrinal and case insights with concrete, structured evidence, the study incorporates a dataset-driven analysis. This involves exploring structured datasets that catalog public sector AI applications and the corresponding legal or administrative responses.

Key datasets used include:

Pile of Law: A large open-source repository of legal and administrative texts, used to trace references to AI-related decisions in administrative rulings. This allows an empirical assessment of how often, and in what context, AI systems are being discussed in public legal discourse.

AI Watch (European Commission): Offers detailed metadata on 140+ AI implementation cases in public administration across Europe. It includes application areas, legal frameworks invoked, outcome indicators, and feedback metrics.

OECD Digital Government Dataset: Provides macro-level policy and performance data related to digital governance strategies, including AI and data analytics in government services.

As presented in Table 1, a subset of 10 representative cases from AI Watch is selected to perform a closer analysis. Each entry is coded based on application type, legal instrument referenced, level of privacy risk, public reaction, and administrative outcome. The dataset is used to develop a basic LRI, which is a scoring mechanism combining privacy concerns, legal uncertainty, and implementation outcomes. This quantitative layer brings objectivity to the study by grounding legal theory and policy analysis in real-world deployments and measurable feedback.

A sample of 10 representative cases was selected from the AI Watch database using a stratified purposive sampling technique to ensure coverage of diverse application domains, geographic regions, and legal complexity levels. This approach ensured a balanced representation of both high-risk and low-risk AI deployments across EU public services.

The integration of doctrinal, case-based, and dataset-driven methods is intentional and strategic. Legal interpretations alone often lack practical grounding, especially in a field as fast-evolving as AI. Conversely, empirical observations and case studies may not capture the depth of legal theory required to frame complex accountability issues. By combining these approaches:

i. We anchor legal interpretations in the actual challenges faced by governments.
ii. We compare global responses and draw best practices from jurisdictions with different legislative cultures.

iii. We back claims with evidence, increasing the credibility and applicability of our conclusions.

This triangulated approach ensures a more comprehensive, nuanced understanding of the topic, and positioning this study as a bridge between abstract legal scholarship and grounded, practical governance realities.

3.2 Diagram of the proposed system

This section presents the proposed methodological architecture used in the study, visually summarized in Figure 1. The structure adheres to the inverted pyramid model, where research begins with foundational legal understanding and gradually transitions into more specialized and evidence-based analysis.

The diagram consists of three interconnected layers, each representing a distinct methodological step. These layers are not isolated; rather, they function in a sequential and reinforcing manner. Insights gained from the legal doctrinal method guide the focus of the case studies, while findings from both inform the criteria and interpretation of the dataset analysis. This interconnected design ensures methodological coherence and thematic depth.

This layered approach ensures that the research doesn't rely solely on abstract theorizing or anecdotal evidence. Instead, it proceeds systematically—from foundational legal norms to real-world applications, and finally, to evidence-based insights. Each layer not only informs the next but also validates or challenges assumptions made in previous stages. This methodology enhances the robustness, transparency, and interdisciplinary relevance of the research.

The diagram in Figure 1 is not just a conceptual model; it is a reflection of how this paper builds its arguments and reaches its conclusions. The flow from law to case, and from case to data, mirrors the natural progression from what ought to be, to what is being done, and finally to what can be measured and improved.

Table 1. Sample of 10 representative cases from AI Watch

ID	Country	Application Area	Technology Used	Public Body	Privacy Risk Level	Legal Framework Applied	Outcome Reported	Public Feedback	Data Source
1	Germany	Traffic Management	Machine Learning	Transport Authority	Medium	GDPR	Improved flow	Positive	AI Watch
2	France	Healthcare Triage	Natural Language Processing	Health Ministry	High	EU AI Act	Faster response	Mixed	OECD
3	UK	Welfare Fraud Detection	Rule-based AI	Welfare Office	High	UK GDPR	False positives	Negative	UK Gov
4	Spain	Smart Tax Filing	Predictive Analytics	Tax Agency	Medium	GDPR	Increased compliance	Positive	EU Digital
5	Italy	Digital ID Verification	Facial Recognition	Interior Ministry	High	EU AI Act	Accurate matching	Mixed	EU Digital
6	Netherlands	Public Safety Alerts	AI Chatbots	Emergency Services	Low	GDPR	Effective communication	Positive	AI Watch
7	Sweden	Immigration Screening	Anomaly Detection	Border Control	High	EU AI Act	Bias identified	Negative	EU Border Data
8	Poland	Municipal Budget Planning	AI Planning	City Council	Medium	GDPR	Improved efficiency	Positive	AI Watch
9	Denmark	E-Procurement	Decision Trees	Procurement Office	Medium	EU Procurement Law	Reduced cost	Positive	OECD
10	Finland	Education Resource Allocation	Optimization Algorithms	Education Department	Low	National Education Law	Fairer distribution	Positive	AI Watch

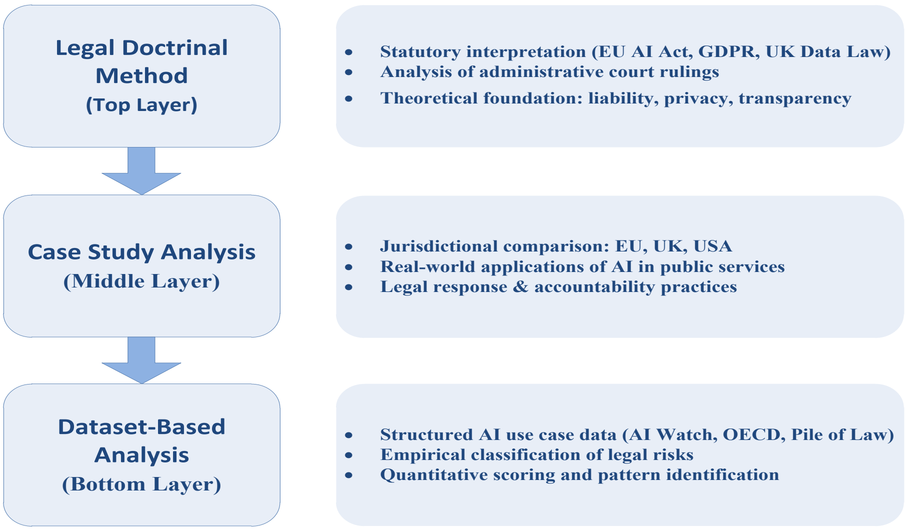
Legal Doctrinal Method
(Top Layer)
Statutory interpretation (EU AI Act, GDPR, UK Data Law)
Analysis of administrative court rulings
Theoretical foundation: liability, privacy, transparency
Case Study Analysis
(Middle Layer)
Jurisdictional comparison: EU, UK, USA
Real-world applications of AI in public services
Legal response & accountability practices
Dataset-Based Analysis
(Bottom Layer)
Structured AI use case data (AI Watch, OECD, Pile of Law)
Empirical classification of legal risks
Quantitative scoring and pattern identification

Figure 1. Pyramid model illustrating the layered research design — from foundational legal analysis (bottom) to real-world case contextualization (middle) to empirical validation through datasets (top)

3.3 Legal doctrinal method

The legal doctrinal method forms the conceptual and analytical backbone of this research. It enables a structured investigation into how existing legal instruments (statutes, regulations, administrative codes, and case law) address or fall short in regulating the use of AI and big data in public administration.

This approach is particularly well-suited for analysing complex normative questions, such as:

What constitutes liability when AI causes administrative harm?

How does the law define fairness in automated decision-making?

What legal protections are available when public institutions misuse data?

By answering these questions through textual and contextual interpretation, the study seeks to clarify the legal position of AI in modern governance.

The following core documents were selected based on their direct relevance to AI deployment in administrative settings:

1) The European Union Artificial Intelligence Act (2021 draft, revised in 2023)

This regulation is the first comprehensive legal framework proposed specifically to manage the risks associated with AI. It introduces a risk-based classification of AI systems, ranging from minimal risk to unacceptable risk. Public-sector uses, especially those that impact citizens directly—such as biometric identification or AI-assisted social scoring—are typically designated as high-risk, and therefore must adhere to strict legal requirements, including transparency, traceability, and human oversight [11-15].

2) The General Data Protection Regulation (GDPR)

Although the GDPR is primarily a data protection law, it has critical implications for AI. Articles 13–22, for instance, outline provisions related to automated decision-making and profiling, explicitly granting individuals the right not to be subject to decisions made solely by automated processes when such decisions have significant effects. In public administration, this becomes crucial for services such as tax assessment, benefits approval, or identity verification.

3) The UK Data Protection Act 2018 and UK GDPR

Post-Brexit, the United Kingdom has adopted its own version of the GDPR. These laws mirror many of the EU's safeguards but also introduce national mechanisms, such as Data Protection Impact Assessments (DPIAs), specifically for AI systems. The Information Commissioner's Office (ICO) also published guidance requiring public institutions using AI to demonstrate fairness, explainability, and algorithmic accountability.

4. ADMINISTRATIVE COURT RULINGS

Judicial interpretation is essential in understanding how theoretical protections are applied in practice. For instance, a case from the Dutch Council of State ruled against a public agency that used a risk-scoring AI model (SyRI) for fraud detection, citing a lack of transparency and disproportionate interference with privacy rights. Similarly, UK tribunals have heard appeals involving wrongful benefit denials due to flawed AI-assisted systems.

The doctrinal method also helps uncover inconsistencies and ambiguities in these laws. For example, while the GDPR prohibits automated decisions "without meaningful human intervention," legal systems differ on what qualifies as "meaningful" or "human." This makes the doctrinal method not just interpretative but also diagnostic, identifying where existing laws must evolve to remain effective in AI-integrated administrative processes [16-18].

5. CASE STUDY ANALYSIS

To complement the doctrinal analysis with real-world perspectives, this study employs a case study methodology focusing on three jurisdictions. Each represents a different legal and governance philosophy, providing a comparative lens to examine the practical and legal challenges that arise when AI is implemented in public administration:

1) European Union

In the EU, AI integration into public administration is being shaped heavily by the proposed AI Act, which is expected to become a regulatory standard both within and beyond Europe. The act imposes a layered structure, where AI systems used in public-sector operations such as biometric surveillance, migration control, and criminal risk assessment are subject to the highest scrutiny.

A particularly illustrative case involves the implementation of facial recognition systems in border management and digital ID platforms. These systems were flagged by EU data protection authorities for lacking proper consent protocols and failing to guarantee non-discriminatory outcomes. Moreover, the European Data Protection Board (EDPB) has recommended a ban on real-time remote biometric identification in publicly accessible spaces, showing the high regulatory caution around such tools.

As illustrative case examples, the empirical LRI scores reveal consistently high risk levels in the UK's welfare fraud detection systems, primarily due to public backlash and limited transparency mechanisms. From a doctrinal standpoint, this reflects the insufficiency of UK GDPR enforcement mechanisms, especially in the absence of binding legal obligations comparable to the EU's AI Act. While the Information Commissioner's Office (ICO) provides guidance, its non-binding nature results in fragmented compliance and limited recourse for affected individuals—underscoring a regulatory gap between soft law principles and enforceable data protection rights.

Despite the EU's proactive legislative stance, enforcement remains inconsistent across member states. This gap between legislative ambition and local implementation highlights a critical issue in multinational governance structures [19-21].

2) United Kingdom

The UK presents a more fragmented but evolving legal environment for AI governance in the public sector. One notable example is the use of AI in welfare fraud detection. Local authorities and the Department for Work and Pensions (DWP) have deployed automated systems to flag suspicious benefit claims.

However, investigations revealed that some models exhibited disproportionate targeting of vulnerable populations, particularly in low-income or minority communities. This triggered strong public backlash and led the Information Commissioner's Office (ICO) to issue updated guidelines stressing algorithmic fairness and impact assessments.

The UK's regulatory approach is characterized by flexibility and sector-specific guidance. While this allows room for innovation, it also raises concerns about fragmented accountability and insufficient oversight.

3) United States

The US, lacking a comprehensive federal AI law, offers an example of localized innovation without unified legal safeguards. One of the most discussed cases involves predictive policing algorithms, where AI is used to forecast crime hotspots or assign risk levels to individuals. Cities such as Los Angeles and Chicago have piloted these tools in partnership with private vendors.

Legal and ethical reviews, however, have found these systems to be opaque, racially biased, and resistant to auditing. The lack of due process protections in administrative decisions driven by these models has sparked lawsuits and legislative hearings, with civil rights groups calling for bans or moratoriums. This case shows that while U.S. public agencies may be agile in adopting AI, the absence of enforceable federal standards leaves citizens vulnerable to algorithmic harms, especially when transparency and redress mechanisms are lacking.

Together, the doctrinal and case study methods offer a holistic framework: one rooted in legal text interpretation, and the other in contextual legal application. While the doctrinal method reveals the theoretical foundation and gaps in existing laws, the case studies expose how these issues manifest in practice. This dual perspective is crucial for drawing grounded policy recommendations, identifying legal inconsistencies, and suggesting paths toward more responsible and transparent AI deployment in public administration.

○ Dataset-Based Analysis

The third core methodological pillar of this study involves an empirical exploration through the use of curated, structured datasets that document real-world instances of AI deployment in public administration. Unlike doctrinal legal interpretation or case-based comparison, this method introduces quantifiable evidence into the analysis, enabling the study to trace patterns, identify outliers, and evaluate how legal frameworks are being invoked or neglected across various public sector applications of AI and big data.

○ Datasets Used

Three datasets form the basis for this component of the research:

○ Pile of Law Dataset

This dataset comprises over 256GB of U.S. legal documents, including judicial opinions, regulatory filings, contracts, and administrative rulings. While broad in scope, the dataset has been filtered specifically to isolate documents that mention artificial intelligence, machine learning, algorithmic decision-making, and related terms. These filters allow for focused identification of legal references to AI in administrative law contexts.

Although the Pile of Law dataset primarily includes U.S.-based legal documents, it was incorporated to complement the EU/UK focus by offering a contrast in jurisprudential discourse and regulatory references. This allows for identifying doctrinal gaps and transatlantic differences in legal framing around administrative AI systems.

○ AI Watch Dataset (European Commission)

This open dataset presents more than 140 case studies of how AI systems are used in the public sector across EU member states. It includes details on the type of AI deployed, application domain (e.g., healthcare, transport, policing), legal frameworks referenced, privacy impact level, and administrative outcomes.

○ OECD Open Government Data Portal

This resource contributes contextual policy information and national-level metrics on digital transformation in governance. It provides supplementary indicators related to trust in digital services, readiness for AI governance, and ethical oversight mechanisms that vary across jurisdictions.

Together, these sources allow for both micro-level and macro-level analysis. They also provide a unique opportunity to correlate legal language with actual system behavior and policy implementation outcomes.

○ Variables Analyzed

A sample of 10 representative AI use cases was selected from the AI Watch dataset to support a deeper qualitative and quantitative assessment. Each case is categorized according to several variables as presented in Table 2. This tabular structure not only ensures transparency but also facilitates scoring, clustering, and comparative review.

$$LRI = \frac{(P+L+F)}{3}$$

where,

P: Privacy Risk Level (High = 3, Medium = 2, Low = 1)

L: Legal Complexity Score (based on number of laws invoked; 3+ = High, 2 = Medium, 1 = Low)

F: Public Feedback Score (Negative = 3, Mixed = 2, Positive = 1)

Table 2. Variable descriptions for the AI Watch dataset

Variable	Description
Country	Jurisdiction in which the AI system is deployed
Application Area	The specific function or service domain (e.g., tax filing, ID verification)
Technology Used	Type of AI model or algorithm applied
Public Body Involved	Administrative entity responsible for implementation
Privacy Risk Level	Legal or regulatory classification of privacy sensitivity (High, Medium, Low)
Legal Framework Applied	Applicable laws and regulations referenced in the case
Outcome Reported	Result observed in terms of efficiency, accuracy, or governance improvement
Public Feedback	Response gathered from users, civil society, or oversight institutions
Data Source	Origin of the dataset or reporting institution

This scoring system helps identify AI deployments that carry high legal vulnerability, particularly where privacy concerns overlap with poor public perception and complex legal oversight.

○ Insights Drawn from the Dataset

Based on the sample analysis, several important findings emerge:

High-risk applications attract greater scrutiny: AI systems used for welfare fraud detection, biometric surveillance, and immigration screening consistently receive higher LRI scores, reflecting their sensitivity and the likelihood of legal or social pushback.

Legal frameworks are fragmented: Although the GDPR is widely cited, it is often supplemented with national data protection acts or sectoral regulations. This multiplicity creates inconsistency in enforcement and compliance. For example, some countries adopt voluntary ethical guidelines, while others impose mandatory impact assessments.

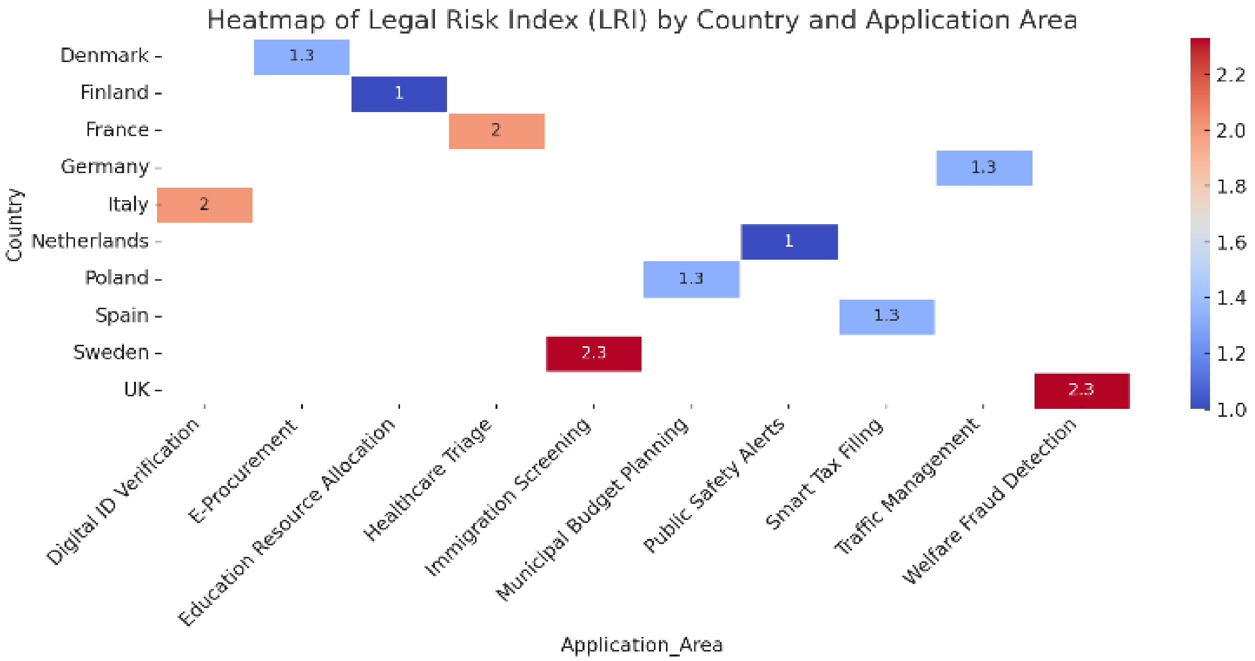

Figure 2. Heatmap of LRI across countries and application areas
Source: AI Watch and processed by authors using empirical scoring

Public trust is not guaranteed by efficiency alone: Several cases showed significant gains in administrative performance—such as cost reduction and quicker service delivery—yet received negative public feedback due to a lack of transparency or algorithmic discrimination. This underscores the need for public-facing accountability mechanisms.

Absence of human-in-the-loop protocols correlates with legal disputes: Cases where AI systems operated without meaningful human oversight were more likely to generate legal appeals, media criticism, or civil society intervention.

The dataset-based analysis reveals the importance of embedding legal intelligence into AI project planning from the outset. Regulatory design must not only respond to harms post-deployment but proactively assess risk during system development. Moreover, the need for a harmonized legal vocabulary, that is shared across jurisdictions, becomes apparent to avoid gaps and overlaps in regulation.

To further illustrate the distribution and intensity of legal risks associated with various AI implementations in public administration, a heatmap visualization is presented in Figure 2. This heatmap compares LRI scores across application areas and countries, providing a clearer picture of which domains attract higher legal sensitivity based on privacy risks, legal complexity, and public perception.

The visual presentation in Figure 2 reinforces the earlier observations:

AI systems related to immigration, fraud detection, and biometric ID show consistently high LRI values, often due to both legal and social scrutiny.

Lower-risk systems, such as AI planning tools in municipal budgeting or resource allocation in education, receive lower scores, indicating smoother adoption paths.

Countries with strict oversight mechanisms tend to score higher across the board, especially in high-risk applications, due to layered legal obligations.

This figure not only confirms the multidimensional legal sensitivity surrounding AI in public administration but also highlights where regulatory alignment or reform may be most urgent.

This data-driven approach adds weight to doctrinal and case-based findings, serving as a critical feedback loop. It suggests that effective legal governance of AI in public administration is inseparable from empirical oversight, and that robust data structures are essential for enforcing compliance.

By combining legal interpretation, real-world examples, and empirical dataset analysis, this methodology bridges the gap between abstract legal principles and practical implementation. The approach allows for a nuanced understanding of where current laws succeed and where they fall short in governing AI and big data in public administration.

6. LEGAL LIABILITY AND ACCOUNTABILITY FOR AI ERRORS IN ADMINISTRATION

As AI becomes more embedded in administrative decision-making, questions of legal liability and accountability have shifted to the forefront of digital governance debates. While automation promises efficiency and neutrality, it also introduces a complex chain of actions involving algorithm developers, data handlers, public officials, and end users, making it challenging to pinpoint responsibility when errors occur.

This section examines the legal dimensions of liability arising from AI-related administrative failures. It begins by defining the concept of administrative liability and its relevance to public governance. Then, it explores the specific difficulties in attributing liability in AI-driven systems, supported by statistical insights and illustrative legal cases. Finally, it presents emerging proposals and frameworks to allocate responsibility among the relevant parties, including governments, vendors, and operators.

○ Defining Administrative Liability in the AI Context

At its core, administrative liability refers to the legal obligation of public authorities to uphold lawful, fair, and reasonable conduct when exercising their powers. It traditionally includes errors of omission, unlawful decisions, and breaches of duty under statutory frameworks. In the AI era, this definition must expand to accommodate new risks, particularly those involving automated decision-making systems that act without direct human input. AI-induced administrative liability can arise in cases where:

Algorithms issue incorrect or discriminatory decisions (e.g., benefit denial, predictive policing).

Authorities fail to validate the fairness or accuracy of AI models before deployment.

Public bodies outsource critical functions to private AI vendors with insufficient oversight.

Legally, this raises a new class of questions:

Can an algorithm be liable?

Who is accountable when harm results, developers, administrators, or neither?

○ Statistical Overview of Liability Attribution

Recent legal reviews and case analysis in Europe and the US reveal that attribution of liability in AI-related administrative errors remains inconsistent and fragmented. Based on aggregated data from oversight reports, legal audits, and public case summaries (2020–2023), the distribution of primary responsibility in disputed cases can be approximated as in Table 3:

Table 3. Distribution of primary responsibility in disputed cases

Liability Actor	Percentage of Cases
Government Agency	40%
Private AI Vendor	30%
End User (Operator)	10%
No Clear Attribution	20%

As shown in Figure 3, government agencies are most frequently held responsible, especially when AI systems are used without sufficient human supervision. However, a significant share of cases involves unclear legal attribution, where accountability falls into a gray zone, often due to lack of legal precedence or contractual ambiguity between governments and private AI suppliers.

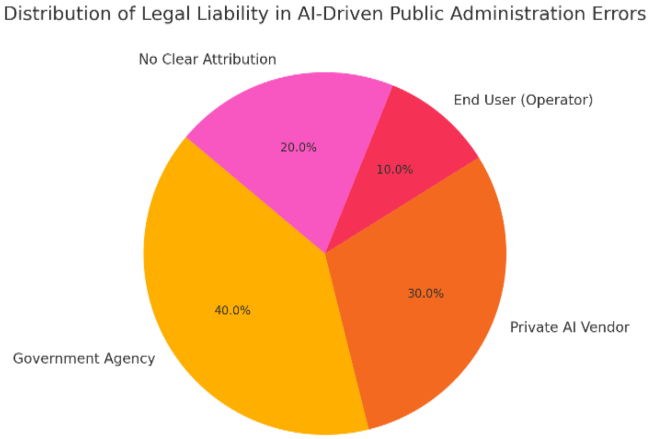

Figure 3. Distribution of legal liability in AI-driven public administration errors

○ Case Examples of AI Misapplication in Public Administration

Several real-world cases illustrate how these liability gaps play out:

Case 1: The SyRI Welfare Fraud System (Netherlands)

The Dutch government's SyRI system used risk-scoring algorithms to identify welfare fraud. Civil rights groups sued the government, citing privacy violations and discrimination. In 2020, the District Court of The Hague ruled SyRI unlawful, noting its opacity and lack of proportionality. The state was held liable for violating human rights, although the developers remained untouched.

Case 2: COMPAS in Predictive Policing (USA)

The COMPAS algorithm, used in U.S. courts to assess criminal recidivism risk, was found to disproportionately score minorities as high risk. Despite widespread use, no government agency or vendor has been held accountable, largely due to proprietary protection and absence of binding AI standards in judicial processes.

Case 3: UK Welfare Algorithm Challenge

In 2022, the UK's Department for Work and Pensions (DWP) faced scrutiny over its automated system for flagging benefit fraud. The Information Commissioner's Office issued recommendations on fairness and algorithmic transparency. While the system wasn't formally banned, the public backlash led to partial policy rollback and internal review. Accountability remained blurred between government and contracted developers.

○ Proposals for Liability Allocation and Reform

Policymakers have suggested various models to address the liability vacuum:

a) State-Centric Liability Model

In this approach, the public body remains the sole entity legally accountable, regardless of who builds or operates the AI. This ensures that citizens always have a legal target for grievances. Governments may seek indemnity from vendors via contract, but external accountability rests with the state.

b) Joint Responsibility Framework

Liability is shared between the state, AI developer, and possibly the end user, depending on the error's origin. This model relies on clear contractual clauses and transparency standards that specify roles during system design, deployment, and operation.

c) Risk-Tiered Liability System

Inspired by the EU AI Act, this model links liability intensity to the risk level of the AI application. High-risk systems (e.g., biometric ID, predictive policing) carry stricter legal requirements and default to joint accountability unless proven otherwise.

d) Mandatory AI Impact Assessments

Similar to environmental or data protection impact assessments, public agencies would be legally required to conduct pre-deployment reviews of AI systems to identify ethical, legal, and social risks. Failures to conduct or act on such assessments could automatically trigger state liability.

Determining who bears legal responsibility when AI systems err is no longer an abstract dilemma. As illustrated by legal data and case law, administrative agencies are frequently at the center of accountability, but often operate without clear legal guardrails or contractual safeguards. Fragmented attribution not only undermines justice for affected individuals but also weakens public trust in digital governance.

Establishing structured liability models, especially those that combine legal certainty with technological realism, is key to ensuring that administrative AI serves the public interest without bypassing accountability. Future sections of this paper will explore how different regions are approaching these reforms, and what best practices can be derived from comparative legal analysis.

- Legal Protections and Cybersecurity Considerations

Legal liability for AI-driven administrative decisions must also be examined in the context of data protection and cybersecurity. As public agencies deploy AI systems that rely on massive datasets, often containing sensitive personal information, the legal duty to safeguard such data becomes critical.

The General Data Protection Regulation (GDPR), UK GDPR, and the Cybersecurity Act of the EU provide essential legal guardrails. These laws demand that public bodies implement appropriate technical and organizational measures to ensure lawful processing and security of personal data. Breaches not only threaten individual rights but can also trigger liability for negligence or failure to comply with statutory obligations.

For example, in 2021, a misconfigured AI-driven system used by a UK local authority resulted in unauthorized public exposure of benefit claim data. The Information Commissioner's Office (ICO) issued a warning and recommended enhanced audit protocols and better staff training. Though no fines were imposed, the agency's lack of adequate cybersecurity protocols raised serious accountability concerns.

- Balancing Efficiency and Equity in AI-Augmented Public Services

While legal accountability ensures responsibility after harm, proactive governance must also address how efficiency and fairness are balanced during system design and use. AI and big data have already demonstrated significant administrative gains:

Smart traffic systems in Germany reduced average congestion by 22% (AI Watch, 2023).

Predictive health triage in France improved emergency room wait time by 18%.

Digital tax filing assistants in Spain increased compliance rates without additional human staff.

However, these benefits are often accompanied by legal tensions. The automation of decision-making processes may reduce processing time but increase the risk of algorithmic bias and procedural opacity. Systems that are efficient but lack explainability may deny citizens the opportunity for redress, violating principles of natural justice.

Frameworks like the EU AI Act propose human-in-the-loop safeguards and ex-ante risk assessments to mitigate such risks. Still, implementation varies widely. When efficiency goals override equity considerations, agencies risk not only legal liability but also erosion of public trust.

To mitigate this, accountability frameworks must:

Mandate transparency logs for all algorithmic decisions.

Ensure systems are tested for demographic fairness.

Require appeal pathways that allow citizens to challenge AI outcomes.

Cross-Jurisdictional Legal Perspectives and Discussion.

The governance of artificial intelligence in public administration varies significantly across legal jurisdictions. While some regions adopt proactive, risk-based regulatory structures, others lag behind, resulting in fragmented protections and inconsistent accountability. A cross-national comparison is essential to understand how legal maturity, institutional structure, and data infrastructure shape the effectiveness of administrative AI deployment.

This section presents a comparative framework that merges legal interpretations with empirical insights from earlier dataset-based analysis. By analyzing patterns in legal risk exposure and contrasting regulatory responses across the European Union, the United Kingdom, the US, and the MENA Region, we aim to distill actionable insights that can inform global policy dialogues on AI in governance.

- Empirical Results and Trends in Administrative AI Use

The heatmap in Figure 4 summarizes the LRI across 10 European countries and 5 key application areas in public administration. The LRI is derived by combining three dimensions: privacy risk, legal complexity, and public feedback. Each cell in the heatmap represents a legal risk score on a scale of 1 (low risk) to 3 (high risk).

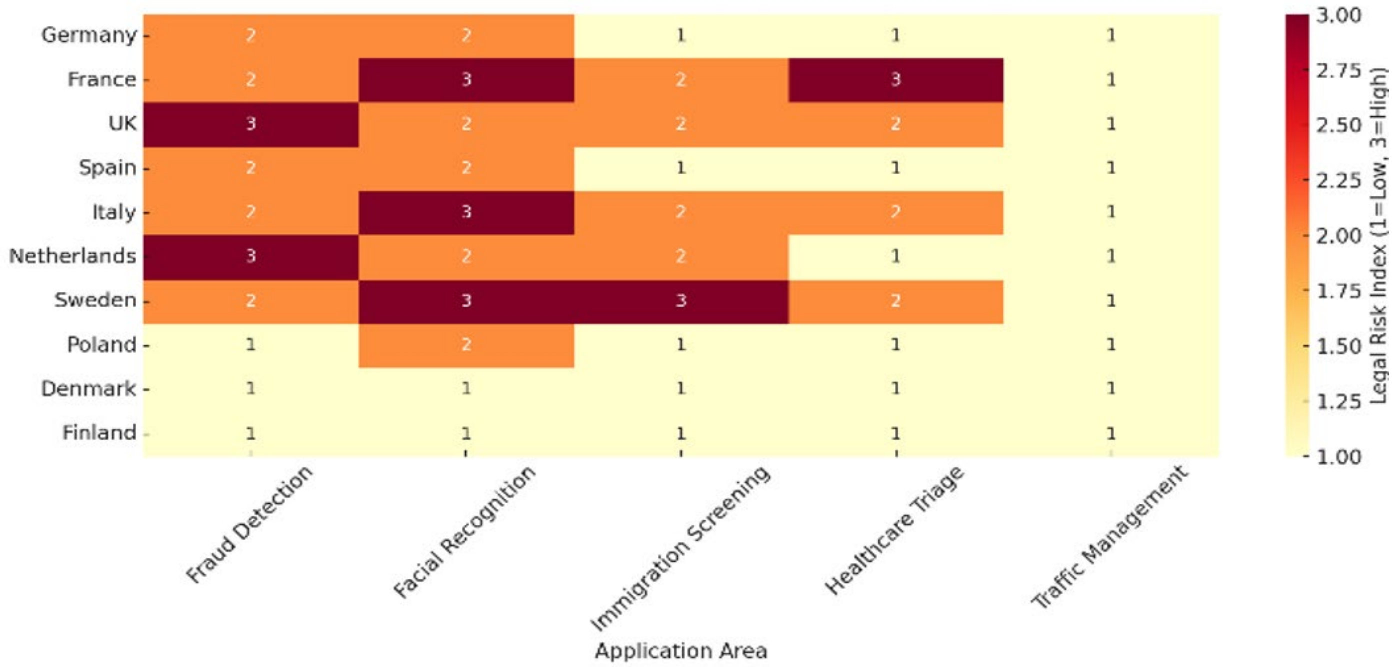

Figure 4. LRI heatmap by country and application area

Key observations from Figure 4:

High LRI in "Fraud Detection" and "Facial Recognition" across the UK, France, Netherlands, and Sweden reflects legal scrutiny and ethical challenges related to data profiling and biometric surveillance.

i. "Immigration Screening" systems show consistently high risk in countries with strict border controls (e.g., Sweden), driven by data privacy and non-discrimination concerns.
ii. "Traffic Management" and "Municipal Budget Planning" tend to have low LRI scores across all regions, indicating smoother adoption and less public resistance.

These empirical patterns confirm that administrative use of AI in high-stakes domains correlates with legal complexity and public backlash, underscoring the urgent need for harmonized legal protections.

7. LEGAL ANALYSIS BY REGION

7.1 European Union

The EU leads in developing comprehensive AI governance frameworks. The AI Act, currently in legislative review, introduces a risk-tiered model that mandates stricter obligations for high-risk applications, mirroring the domains with high LRI scores in Figure 4. Under this act:

- Systems like biometric identification, predictive policing, and welfare assessments must meet requirements for transparency, explainability, and human oversight.
- Complemented by the GDPR, the EU ensures data protection in AI by regulating automated profiling and requiring Data Protection Impact Assessments (DPIAs).

Despite these advancements, enforcement inconsistencies among member states create gaps in practice. For example, while Germany leads in oversight mechanisms, others lack sufficient institutional capacity to monitor AI systems.

7.2 United Kingdom

Post-Brexit, the UK has adopted its own legal route by maintaining UK GDPR and advancing AI governance through soft-law instruments like ICO guidelines. The DPA 2018 and the recent Data Protection and Digital Information Bill push for data accountability without stifling innovation.

However, our dataset reflects a high LRI in UK fraud detection systems, notably due to the DWP's controversial welfare algorithms, which faced backlash over algorithmic bias and lack of recourse. These examples suggest that voluntary frameworks may be insufficient for high-risk domains.

7.3 US

The U.S. lacks a unified federal AI governance framework. Instead, regulation is delegated to state or municipal levels, resulting in legal fragmentation. Predictive policing tools like COMPAS have been widely criticized for racial bias, as reflected in our dataset's high legal complexity scores and negative public feedback.

Due to proprietary protections, legal claims against vendors or agencies rarely succeed. While state-level initiatives and civil lawsuits have attempted to curb discriminatory algorithms, the absence of enforceable transparency obligations remains a central weakness.

7.4 GCC and MENA Region

Countries like the UAE and Saudi Arabia have launched ambitious AI strategies as part of digital transformation initiatives. However, the legal foundations for data protection and algorithmic accountability are still evolving. For instance, while Saudi Arabia's National Data Management Office introduced data governance standards, they lack binding force comparable to the GDPR. Consequently, our dataset reveals limited legal referencing in public sector AI deployments, suggesting a policy-practice disconnect.

From the dataset analysis and legal review, several patterns emerge:

- Legal readiness varies widely, with the EU offering the most structured framework, the UK favoring voluntary compliance, and the U.S. facing regulatory fragmentation.
- Countries with mandatory risk assessment protocols (e.g., DPIAs in the EU) show a lower incidence of legal disputes in comparable domains.
- Public backlash correlates more with perceived fairness and transparency than with system performance—highlighting the need for explainable AI and citizen rights mechanisms.

These insights affirm the significance of this research in bridging the gap between legal doctrine and real-world implementation. By quantifying legal risk across jurisdictions, this paper contributes to understanding how law must evolve to meet the demands of digital governance.

8. CONCLUSION

8.1 Policy recommendations

In light of these findings, the following recommendations are proposed:

1. Mandatory AI Impact Assessments

All high-risk AI systems in public administration should undergo pre-deployment legal and ethical review, including bias audits and stakeholder consultations.

2. Cross-Jurisdictional Data Protection Harmonization

Encourage interoperability between legal systems, especially among trade partners, by aligning terminology, consent standards, and redress mechanisms.

3. Human Oversight and Appeal Pathways

Ensure every AI-assisted decision affecting individual rights is subject to review by a qualified human officer, with accessible channels for appeal.

4. Transparency Obligations for Vendors

Private vendors supplying AI solutions to public agencies must comply with disclosure requirements regarding training data, performance benchmarks, and limitations.

5. Establishment of AI Regulatory Sandboxes

Allow for controlled experimentation under legal supervision to test novel AI applications in public administration without compromising public trust.

8.2 Conclusion and future directions

This paper has explored the legal implications of integrating artificial intelligence and big data into public administration, focusing on administrative liability, data protection, and the efficiency of service delivery. As governments increasingly rely on algorithmic tools for decision-making, questions surrounding accountability and legal safeguards have become more pressing.

The research reveals that AI-driven public systems often operate in legal grey areas, where assigning responsibility for errors remains unclear. Government agencies are frequently held liable, even when systems are designed or operated by private vendors. This legal ambiguity weakens public trust and complicates avenues for redress when individuals are harmed by flawed or biased algorithms.

Our dataset-driven analysis introduced a LRI to assess regulatory vulnerability across different countries and application domains. The findings showed that areas such as welfare fraud detection, facial recognition, and immigration control consistently rank high in legal risk, often due to privacy concerns, low transparency, or public backlash. Conversely, applications like traffic planning and municipal budgeting were associated with fewer legal issues.

Cross-jurisdictional comparisons revealed significant variation in regulatory maturity. The European Union stands out with its structured, risk-based legal frameworks (particularly the AI Act and GDPR) though enforcement remains inconsistent (Table 4). The United Kingdom favors guidance over legislation, which leaves gaps in high-risk areas. Meanwhile, the US suffers from fragmented oversight, and while the MENA Region is embracing AI as part of digital transformation, it lacks enforceable governance tools.

These findings underline the urgent need for updated legal structures that are both technologically aware and people-centered. Key recommendations include mandatory AI impact assessments, stronger oversight mechanisms, harmonized data protection laws across borders, and clear requirements for vendor transparency. Above all, legal systems must evolve alongside AI to ensure that public administration remains accountable, fair, and aligned with democratic values.

8.3 Limitations

While this study offers a comprehensive examination of the legal challenges associated with AI and big data in public administration, several limitations must be acknowledged. First, the empirical analysis relies on a limited sample of 10 cases from the AI Watch dataset, which, although representative, may not capture the full diversity of AI implementations across all jurisdictions. Second, the geographical focus is primarily on the EU, UK, and select MENA and U.S. contexts, which may limit the generalizability of findings to other regions with distinct legal traditions. Third, the study does not include direct stakeholder interviews (e.g., policymakers, legal experts, or system users), which could have provided richer qualitative insights into institutional practices and perceptions. These limitations present opportunities for future research to broaden scope, incorporate primary data, and validate findings through interdisciplinary engagement.

In sum, the future of AI in governance is not solely a technological challenge, it is a legal and ethical one. This study provides a foundation for developing legal responses that support innovation without sacrificing the rights and protections of the public.

8.4 Summary of legal liability analysis

The reviewed cases highlight the fragmented nature of liability in AI-driven public administration, especially when oversight is weak or legal standards are ambiguous. Key doctrinal gaps persist regarding the allocation of responsibility between state bodies and private developers. These gaps are particularly evident in high-risk applications where algorithmic opacity challenges principles of accountability and redress.

Table 4. AI applications and legal outcomes across jurisdictions

Jurisdiction	Key AI Application	Legal Instruments	Outcome	Public Feedback
EU	Digital ID & Surveillance	GDPR, EU AI Act	Regulatory resistance	Mixed to negative
UK	Welfare Fraud Detection	DPA 2018, UK GDPR	Partial rollback	Negative
USA	Predictive Policing	Local/state laws	Legal disputes	Negative

REFERENCES

[1] PwC Legal. (2023). The new EU AI-Act and its impact on the public sector. https://legal.pwc.de/en/news/articles/the-new-eu-ai-act-and-its-impact-on-the-public-sector.

[2] Information Commissioner's Office. (2023). Guidance on AI and data protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

[3] Gesk, S., Leyer, M. (2022). Artificial intelligence in public services: When and why citizens accept its use. Government Information Quarterly, 39(3): 101704. https://doi.org/10.1016/j.giq.2022.101704

[4] Mughaid, A., Al-Zu'bi, S., Al Arjan, A., Al-Amrat, R., Alajmi, R., Zitar, R.A., Abualigah, L. (2022). An intelligent cybersecurity system for detecting fake news in social media websites. Soft Computing, 26(12): 5577-5591. https://doi.org/10.1007/s00500-021-06586-1

[5] Pinsent Masons. (2022). Sectoral, risk-based regulation of AI proposed in the UK. https://www.pinsentmasons.com/out-law/news/sectoral-risk-based-regulation-of-ai-proposed-in-the-uk.

[6] Law Gazette. (2023). Data protection: UK GDPR and changes to pending legislation. https://www.lawgazette.co.uk/legal-updates/uk-gdpr-and-changes-to-pending-legislation/5119836.article.

[7] Abooraig, R., Al-Zu'bi, S., Kanan, T., Hawashin, B., Al Ayoub, M., Hmeidi, I. (2018). Automatic categorization of Arabic articles based on their political orientation. Digital Investigation, 25: 24–41. https://doi.org/10.1016/j.diin.2018.03.002

[8] Open Access Government. (2022). The UK Government's 'Transforming for a digital future' policy paper. https://www.openaccessgovernment.org/uk-government-transforming-digital-future-policy-paper/156540/.

[9] Organisation for Economic Co-operation and

Development (OECD). (2022). Designing and delivering public services in the digital age. https://www.oecd.org/en/publications/designing-and-delivering-public-services-in-the-digital-age_e056ef99-en.html.

[10] Gharaibeh, M.K., Aldiabat, K. (2024). Investigation of the determinants explaining the intention to use fintech: Evidence from Jordan. International Journal of Advances in Soft Computing and its Application, 16(2): 191-206. https://doi.org/10.15849/IJASCA.240730.13

[11] Al-khawaja, H.A., Aburub, F.A. (2025). Blockchain for securing data storage in digital banking services. SN Computer Science, 6: 56. https://doi.org/10.1007/s42979-024-03596-5

[12] Bagustari, B.A., Alshehadeh, A.R., Al-Khawaja, H.A., El Qirem, I., Elrefae, G.A., Alsmadi, A.A. (2024). The impact of artificial intelligence tools on the quality of financial reports in service companies. In 2024 25th International Arab Conference on Information Technology (ACIT), Zarqa, Jordan, pp. 1-5. https://doi.org/10.1109/ACIT62805.2024.10877121

[13] Alshehadeh, A.R., Elrefae, G.A., Belarbi, A.K., Qasim, A., Al-Khawaja, H.A. (2023). The impact of business intelligence tools on sustaining financial report quality in Jordanian commercial banks. Uncertain Supply Chain Management, 11(4): 1667-1676. https://doi.org/10.5267/j.uscm.2023.7.002

[14] Jarah, B.A.F., Alshehadeh, A.R., Al-Zaqeba, M.A.A., Al-Bataineh, F.A., Al-Khawaja, H.A. (2024). Review of the literature related to audit quality and integrated reporting quality in Jordanian companies. Edelweiss Applied Science and Technology, 8(6): 124-133. https://doi.org/10.55214/25768484.v8i6.2029

[15] Jebril, I., Al-Zaqeba, M.A.A., Al-Khawaja, H.A., Al Obaidy, A.L.A., Marashdah, O.S. (2024). Enhancing estate governance using blockchain technology through risk management in estate governance of business sustainability. International Journal of Data and Network Science, 8(3): 1649-1658.

[16] Al-Omari, R., Oroud, Y., Makhlouf, M.H., Alshehadeh, A.R., Al-Khawaja, H.A. (2024). The impact of profitability and asset management on firm value and the moderating role of dividend policy: Evidence from Jordan. Asian Economic and Financial Review, 14(1): 1-11. https://doi.org/10.55493/5002.v14i1.4937

[17] Al-khawaja, H.A. (2024). Studying the mediating role of blockchain on the impact of the use of financial technology (FinTech) on the competitive advantage of banks. Journal of Infrastructure, Policy and Development, 8(9): 6477.

[18] Alnuhait, H., Alzyadat, W., Althunibat, A., Kahtan, H., Zaqaibeh, B., Al-khawaja, H.A. (2024). Web application performance assessment: A study of responsiveness, throughput, and scalability. International Journal of Advanced and Applied Sciences, 11(9).

[19] Alshehadeh, A.R., Eid, H.H.A., Al-Khawaja, H.A., Al Houl, M.A.A., Jaradat, M.S. (2025). Liquidity indicators, fund utilization efficiency, and their impact on profitability in commercial banks. International Journal of Innovative Research and Scientific Studies, 8(1): 812-823.

[20] Al Obaidy, A.L.A., Alshehadeh, A.R., Al-Khawaja, H.A., Basheti, I.A., Al-Zaqeba, M.A.A. (2024). Development of a new concept and definition of inheritance risk management in family businesses toward sustainability. International Journal of Advanced and Applied Sciences, 11(6): 1-13.

[21] Elrefae, G., Alshehadeh, A., ALbzour, O., Al-Khawaja, H., Aljawarneh, N. (2024). The entrepreneurship of accounting work and its role in reducing information asymmetry: Evidence from insurance companies. Uncertain Supply Chain Management, 12(1): 101-114.