TPM Vol. 31, No. S2, 2024
ISSN: 1972-6325
https://www.tpmap.org/

ARTIFICIAL INTELLIGENCE, CYBER LAW, AND DATA PROTECTION: LEGAL CHALLENGES AND REGULATORY RESPONSES IN THE DIGITAL AGE

[1]ASIA RAHMAN KHAN LODHI, [2*]AHMAD SAJJAD, [3]KASHIF AKBAR, [4]DR SYED SHUJA UDDIN, [5]DR. RIZWANA JABEEN, [6]AZHAR HUSSAIN LASHARI

[1]DY. DIRECTOR DEPARTMENT: MINISTRY OF INFORMATION & BROADCASTING, ISLAMABAD, ASIA.KHAN.LODHI@GMAIL.COM
[2]NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ASAJJAD@ACAE.NUST.EDU.PK
[3]DEPARTMENT OF INDUSTRIAL ENGINEERING, UNIVERSITY OF PADUA, ITALY, KASHIF.AKBAR@STUDENTI.UNIPD.IT
[4]ASSISTANT PROFESSOR, DEPARTMENT OF INTERNATIONAL RELATIONS, FEDERAL URDU UNIVERSITY OF ARTS, SCIENCES & TECHNOLOGY, KARACHI, PAKISTAN, DR.SHUJA.IR@FUUAST.EDU.PK, HTTPS://ORCID.ORG/0009-0008-8359-9915
[5]ASSISTANT PROFESSOR DEPARTMENT OF INTERNATIONAL RELATIONS FEDERAL URDU UNIVERSITY ART'S SCIENCE AND TECHNOLOGY, KARACHI, PAKISTAN, RIZWANAJABEENDR@GMAIL.COM
[6]LECTURER COMPUTER SCIENCE, COLLEGE EDUCATION DEPARTMENT GOVT. OF SINDH, LASHARIAZHAR@GMAIL.COM

ABSTRACT
The swiftly expanding use of artificial intelligence in the commercial, governmental, and social spheres has created a multi-layered and dynamically changing complex of legal issues at the boundary of cyber law, data protection, and algorithmic governance. This paper is based on a qualitative research design with an interpretivist paradigm to explore how legal frameworks, regulatory authorities and governance institutions are adapting to the legal challenges of AI-driven data processing, automated decision-making, cybersecurity threats, and the loss of conventional structures of individual privacy and data sovereignty. Based on purposive sampling, 25 key informants, such as legal professionals specializing in cyber and data protection law, cybersecurity professionals, national and international policymakers, and IT regulators, took part in semi-structured, in-depth interviews. These topical reports were cross-referenced with systematic document analysis on national cyber laws, data protection laws, case law and international regulatory frameworks such as the EU General Data Protection Regulation (GDPR), the EU Artificial Intelligence Act (2024), the California Consumer Privacy Act (CCPA), China Personal Information Protection Law (PIPL), India Digital Personal Data Protection Act (DPDPA 2023), and other similar national laws. Thematic analysis produced six main themes that include privacy and data rights in AI systems, accountability and transparency of algorithms, cybersecurity and data breach liability, legal gaps and jurisdictional conflicts, regulatory responses to AI emerging, and the implications of generative AI to intellectual property. Results indicate that there is a systemic regulatory deficiency in most national jurisdictions in dealing with the unique legal issues associated with AI-driven systems, with failures in consent architecture, lack of explainability, cross-border jurisdictional issues, and the novel legal issues of generative AI all contributing to exposing critical failures in current legal and regulatory regimes. The most substantive existing attempt to regulate AI-specific legal issues is the European Union AI Act, although much remains unclear about its implementation. The research closes by giving suggestions to legislators, regulatory authorities, international governance bodies, and technology companies involved in creating and implementing AI systems under the modern legal and ethical systems.

KEYWORDS: artificial intelligence, cyber law, data protection, GDPR, EU AI Act, algorithmic accountability, privacy, digital governance, regulatory frameworks, qualitative research, data sovereignty, generative AI.

INTRODUCTION

The rise of artificial intelligence as an all-encompassing organizing technology to modern economic, social and governmental life has brought about a significant and increasing conflict between the disruptive potential of AI

systems and the legal frameworks that have traditionally regulated the gathering, processing, and use of personal data. This stress point is acute where three interrelated fields are at issue: artificial intelligence - the entire body of legal doctrine that regulates the behavior of digital environments, including cybersecurity requirements, regulation of electronic commerce, generation of digital evidence, and jurisdiction issues in cross-border digital settings; cyber law - the body of legal doctrine that regulates the behavior of digital settings, such as cybersecurity requirements, regulation of electronic commerce, generation of digital evidence, and jurisdiction in The speed of co-evolution of these three areas, already extremely complicated on their own, poses a challenge of governance of unusual complexity, which current legal frameworks are already showing that they are failing to overcome (Doshi-Velez et al., 2017).

The magnitude and speed of data processing that is produced by AI in modern digital contexts cannot be easily understood. The total size of global digital data creation is rated at 120 zettabytes in 2023, and AI systems are becoming an increasingly key source of the production and processing of this enormous informational resource (Statista, 2024). The biggest AI models being trained today consume hundreds of billions of data points scraped off the open web, social media, academic literature, and digitized literature and artistic collections - casting fundamental challenges to the legality of this massive-scale harvesting of human-generated information within intellectual property and data protection laws that were originally created in a different technological era altogether. During deployment, AI systems handle personal data at rates and scales inaccessible under current consensual-based data protection regimes to meaningfully control individuals in the first place, creating a structural imbalance between legal theory and technological practice that is the hallmark of modern data protection legislation.

The cybersecurity aspect of such a challenge is no less deep. Both defenders and attackers are equally increasing their capabilities with AI technologies, creating a technological arms race in which AI-driven offensive capabilities, such as automated vulnerability exploitation, AI-generated phishing attacks, deepfake social engineering attacks, and adversarial machine learning attacks on security systems, are outpacing the defensive cybersecurity framework and legal liability regime built in a digital security contest dominated by human adversaries (Brundage et al., 201 The legal issues that have always complicated the law of cybersecurity are just being multiplied by the fact that attacks, in which the AI systems are designed, executed and obscured, are happening across and between jurisdictions - making the already problematic legal frameworks of state responsibility, corporate liability and individual criminal responsibility increasingly ineffective in regulating the AI-enhanced cyber threat environment. The underlying issues concerning the legal personality of AI, such as the ability to hold an AI system accountable due to its results and who is liable when an AI system is involved in causing harm, are not addressed by most legal systems, creating a lot of uncertainty in the application of AI in high-stakes decision-making scenarios such as employment screening, credit evaluation, healthcare diagnosis, criminal justice, and social welfare provision (Doshi-Velez et al., The first major attempt to impose a legislative limit on the power of an algorithm to make decisions was the right to explanation of the GDPR in Article 22, the right not to be subjected to a purely automated decision that could have a significant impact on it, and the right to obtain a meaningful explanation of the logic of that decision, which has been hindered due to the lack of transparency in the internal decision-making mechanisms of modern deep learning systems,The global regulatory trends in 2024 have greatly transformed the legal environment on AI regulation. The Artificial Intelligence Act of the European Union - legally binding since August 2024 - is the first legal framework in the world that is specifically created to control AI systems, based on their risk potential, and creates a tiered regulation framework between banned AI applications (and real-time biometric surveillance of public areas and social scoring) by high-risk uses that need conformity assessment (such as AI in the workplace, credit, law enforcement, and critical infrastructure) to lower-risk uses that have transparency requirements (Floridi et al., 2018). The possible impact of the EU AI Act as a global regulatory model, emulating the GDPR-style "Brussels Effect" of having its terms and conditions adopted as a de facto international standard, means that its provisions and problem areas of implementation are issues of global regulatory importance that reach well beyond European countries.

The motivation of this study was the seemingly existing gap between the rate of AI-related legal challenges and rates of scholarly legal responses establishing the legal challenges on the experience of those who work with them daily, i.e., lawyers, regulators, cybersecurity workers, and policymakers. Although there is a massive and expanding normative and doctrinal literature on AI governance, the qualitative empirical research on how legal and regulatory professionals perceive, negotiate, and attempt to resolve the unique legal issues of AI systems is relatively scarce. The practitioner insights evoked by the qualitative methodology of this study offer both confirmatory richness and critical sensitivity to the particular legal issues and regulatory reactions that theoretical frameworks recognize and provide a practical aspect of implementation and enforcement, which theoretical analysis might not necessarily be able to envision.

The research was conducted by semi-structured interviews with 25 purposely chosen expert respondents - who worked in cyber law practice, data protection regulation, cybersecurity operations, national and international policy-making, and academic legal scholarship - as well as in-depth documentary research on primary legal sources such as statutes, regulations, court decisions, regulatory guidance, and international framework instruments. The results, presented in the form of thematic analysis as six main themes, give a multi-perspectival and comprehensive picture of the current situation and developmental trajectory of AI, cyber law, and data protection governance that has substantial

implications on legal scholarship, regulatory design, corporate compliance, and the development of international governance institutions.

The article continues in the following manner. Section 2 provides a review of the theoretical and doctrinal basis literature in the major thematic areas of the study. Section 3 discusses the research methodology. Section 4 presents thematic results, which are backed by two analysis tables. Section 5 presents conclusions in terms of theory and policy. Recommendations are provided in section 6. The article has been organized in a way that is not only comprehensible to a legal expert, but also to an interdisciplinary audience due to the nature of subject that is inherently cross-disciplinary.

A terminological caveat: in this article, the term artificial intelligence is applied in its broadest sense of any machine learning-based system such as predictive analytics, large language models, generative AI, computer vision and autonomous systems, following the definition in the EU AI Act. The term 'data protection' is employed to refer to both the technical subdivision of the regulation of personal data privacy and to the general issue of individual rights in the face of digital surveillance and exploitation of data. Cyber law is applied in its most extensive sense to refer to all legal doctrine pertaining to digital environments, communications and transactions.

2. LITERATURE REVIEW

2.1 The Legal Architecture of Data Protection: GDPR to the Global Proliferation of Regulations

The legal regulation of personal data has changed to a patchwork of sectoral and national privacy regulations, beginning with the European Convention on Human Rights Article 8 right to private life and replicated into data protection laws by the Hessische Datenschutzgesetz of 1970 in Germany, the first data protection law in the world, to a network with more and more interconnected and globally influential regulatory provisions anchored in the General Data Protection Regulation of the The GDPR, coming into force in May 2018, introduced a complete set of data subject rights, data controller and processor responsibilities, and enforcement powers of supervisory authorities in a new form of data protection law in Europe since the 1995 Data Protection Directive, and quickly became the de facto international standard of data protection legislation.

The substantive architecture of the GDPR is based on 6 principles of lawful data processing, namely, lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and provides data subjects with a series of rights, such as access, rectification, erasure, restriction, portability, and objection (Voigt and von dem Bussche, 2017). The extraterritorial application in the regulation, contained in Article 3, paves its way to the jurisdiction of any organization, no matter where it is based, which provides goods or services to EU data subject or tracks their activities, making the international technology industry subject to the global compliance standards of GDPR and creating the so-called Brussels Effect of the global adoption of GDPR compliance standards by multinational corporations.The adequate decision framework of the GDPR, capping the transfer of personal data to third countries unless the data protection standards are deemed to be adequate, has caused a lot of geopolitical tension especially within the framework of EU-US data transfer agreements. The Court of Justice of the European Union decisions of Schrems I (2015) and Schrems II (2020) gradually tightened the limitations on EU-US data delivery, discovering that the Safe Harbor and Privacy Shield models were inefficient to safeguard European personal data against intelligence surveillance measures in the U.S. The third effort to create a viable adequacy arrangement is the EU-US Data Privacy Framework, which was adopted on July 2023, but which legal commentators have found inadequate in terms of its oversight mechanisms to address the underlying CJEU issues that had undermined its predecessors (Kuner, 2020).The universal expansion of the data security laws after GDPR has been impressive both in magnitude and geographic coverage. By 2024, more than 160 countries have passed broad data protection laws or meaningful sector privacy laws, an incredible growth of about 50 countries in 2000 (UNCTAD, 2024). Global: India has adopted a Digital Personal Data Protection Act (2023), Brazil has adopted the LGPD (2020), South Africa has adopted the POPIA (2021), China adopted the PIPL (2021), and Pakistan is proposing a Data Protection Bill which all reflect a regulatory convergence around GDPR-inspired principles of consent, purpose limitation, data minimization, data subject rights, but vary widely

2.2 Artificial Intelligence Regulation: Concepts, Threats, and the EU AI Act

Artificial intelligence governance has been quickly gone up the academic marginal preoccupation ladder to the mainstream preoccupation of international policy discourse -profile AI-driven discrimination, surveillance overreach, disinformation generation and autonomous weapons development that have all shown the possibility of the AI system to inflict systemic social harm at an unprecedented scale and speed (Doshi-Velez et al., 2017). The literature on regulatory efforts has converged around a set of principles of governance - transparency, explainability, fairness, accountability, human oversight, privacy and safety - which indicates a broad normative consensus on the desiderata of responsible AI-based systems but varies widely in how they are operationalized within a range of institutional and national regulatory frameworks.

The EU Artificial Intelligence Act is the most substantive legislative effort to express these principles of governance into binding regulatory requirements. The AI Act implements a risk-based regulatory framework, dividing risks into

four categories: prohibited AI systems (such as real-time biometric identification in the public, AI in critical infrastructure, education, employment, required access to necessary services, law enforcement, migration, and administration of justice); high-risk AI systems (including AI in critical infrastructure, education, employment, required access to essential services, law enforcement, migration, and administration of justice); limited-r.

The General Purpose AI (GPAI) provisions of the AI Act, which came about due to a rush to enact the legislation in response to the sudden proliferation of foundation models such as ChatGPT, Gemini, and Claude, place extra obligations on the providers of GPAI models, such as disclosure of training data, documentation of compliance with copyrights, and increased responsibilities on GPAI models determined to have systemic risk (such as These provisions form the initial legislative effort to enforce foundation model providers as a specific type of AI actor, but serious doubts exist regarding their technical operationalizability, as well as the sufficiency of the compliance infrastructure that will be necessary to realize them on a large scale.

Outside the EU model, national AI policy regimes differ significantly in terms of institutional structure and content. The United States has been largely an executive and agency-led strategy, and the Executive Order on AI Safety issued by the Biden administration (October 2023) instructs agencies to develop industry-specific AI principles and sets reporting obligations in frontier AI model development. The NIST AI Risk Management Framework is a voluntary framework of governance of AI risk assessment and management, although the lack of federal AI legislation leads to a disjointed regulatory landscape where AI governance requirements differ greatly across industry sectors, state jurisdictions, and deployment contexts (Brundage et al., 2018). The AI regulatory strategy in China is based on a combination of extensive regulation of particular areas of AI applications e.g. algorithmic recommendation systems (2022), deep synthesis technologies such as deepfakes (2022), and generative AI services (2023) and fits within a larger persona of a state-led AI industrial policy that places an emphasis on AI leadership and security and on individual rights concerns.

2.3 Cyber Law Cybersecurity Obligations,and the Evolving Threat Landscape

The scope of cyber law includes the legal regulations of digital-environment behavior, such as cybercrime law, electronic commerce law, cybersecurity law, the rules of digital evidence, and the international law aspect of state behavior in cyberspace. Budapest Convention on Cybercrime (2001) has formed the basis of international cooperation in cybercrime, with definitions of computer-related crimes and guidelines on international evidence-sharing and extradition, which have been embraced by more than 60 states (Council of Europe, 2001). But even the scope of AI-enhanced cyber threats addressed by the Convention, such as AI-driven malware, automated social engineering, and automated attacks on AI systems, is practically zero, with this scope reflecting the technological horizon of the time of drafting in 2001.

The EU Network and Information Security Directive (NIS2, 2022) has drastically changed the legal and regulatory environment concerning cybersecurity and has increased the number of critical infrastructure sectors subject to mandatory cybersecurity requirements and added greater incident notification requirements and shorter notification deadlines than its predecessor. The interplay of NIS2 with GDPR presents organizations that have suffered cybersecurity incident involving personal data with a dual compliance requirement, that is, not only 72-hour data breach notification requirements under GDPR Article 33, but also with independent NIS2 notification requirements, with different timeframes, different addressee requirements, and different information requirements. Legal practitioners have found this regulatory complexity to cause considerable compliance management difficulties, especially in small organizations that lack legal and cybersecurity compliance departments.The liability aspect of cybersecurity law is especially tricky in the case of AI-enhanced threats. The current product liability systems, such as the Product Liability Directive of the EU (revised in 2024) and similar national systems, find it difficult to adapt to the distributed nature of causation, autonomous system functionality, and software-specific nature of AI-driven cyberattacks. Whether AI systems are products on product liability grounds, and whether the primary responsibility to take legal action against harm caused by AI system failure lies with the producers, deployers, or operators of the affected AI systems, is a contentious issue across jurisdictions - creating a liability gap that may not sufficiently incentivize investment in AI system security (Calo, 2017).

2.4 Algorithmic Accountability, Automated Decision-Making

Law The legal regulation of automated decision-making systems, including credit score systems and employment screening systems, as well as predictive policing tools and systems to determine eligibility to social welfare, have become some of the most practically consequential areas of AI law, owing to the direct and frequently devastating effects of algorithmic decisions on individual life opportunities, civil rights, and human dignity. Doshi-Velez et al. (2017) offer a legal framework of the transparency requirements of machine learning systems by distinguishing between technical explainability, the extent to which the inner workings of a system can be characterized, and legal explainability, the extent to which the decisions of a system can be interpreted and examined in a legal context by the courts, regulators, the people who were affected, and their legal representatives.

An automated decision-making clause in GDPR and specifically the right not to be the subject of merely automated individual decision-making with serious legal consequences in Article 22 of the GDPR alongside the right to meaningful information about the logic behind such decisions in the same article was the first major effort of law to

introduce explainability requirements to algorithmic decision systems. Nevertheless, the reality of applying these provisions has been highly problematic: due to the technical complexity of the modern machine learning systems, the provision of meaningful information about the logic behind the operation is immensely challenging in a form understandable by lay people, and the legal standard of meaningful information has not been well defined to offer a clear guide to organizations that use automated decision systems.

Recent work on algorithmic fairness has cast basic doubts on the connection between statistical optimization and legal non-discrimination principles. The mathematical infeasibility of achieving multiple often-used definitions of algorithmic fairness, such as equal accuracy rates between groups, equal false positive rates, and equal predictive value, has important consequences in the legal regulation of AI systems in anti-discrimination law settings (Barocas et al., 2019). In the United States, the United Kingdom and in European Union courts, automated decision accountability has started to take shape as courts initiate a nascent jurisprudence of algorithmic decision accountability, which will inform the legal landscape of algorithmic system in high-stakes decision contexts over decades.

3. METHODOLOGY

3.1 Research design and Epistemological framework

This paper embraced a qualitative research design based on an interpretivist research paradigm. Interpretivist approach acknowledges that law and regulatory phenomena as understanding of legal problems, interpretation of regulatory requirements, and design of governance reactions are inherently constructed by the professional knowledge, institutional experience, and interpretativeness of practitioners who operate with them (Denzin and Lincoln, 2018). The expert interpretations of AI by legal and regulatory practitioners are not ready-made interpretations of what can be found in objective legal texts; they emerge through the influence of professional training, institutional location, case law, jurisdiction and the specific technological and regulatory dynamics of the practice of the practitioner. To capture this richness of interpretation, a qualitative inquiry is necessary that is capable of capturing contextual nuance, professional variation and the complexity of expert judgment in a manner that cannot be recreated using survey-based methods or quantitative techniques.

The exploratory aspect of the design recognizes the quickly changing nature of the topic. The legal issues surrounding AI are truly new in most aspects, the introduction of the EU AI Act in August 2024 is only a few weeks old when this paper was written, and the legal theory of AI-related issues is still in its infancy. Exploratory qualitative inquiry is tailored to emergent phenomena in which the main scholarly goal is the production of deep descriptive and analytical knowledge as opposed to the test of a set of theoretical propositions, which situates it methodologically well to the current phase of AI law and governance research.

3.2 Purposive sampling and profile of participants

The participants were recruited using a purposive sampling approach to select those who had direct, relevant expertise in the legal, regulatory and technical aspects of the subject of the study. The recruitment criteria focused on depth and diversity of expertise in five areas of professional practice: cyber and data protection law practitioners with active practice in advisory or litigation; cybersecurity professionals with experience in organizational risk management and incident response in data-intensive settings; national and international policymakers with direct experience in AI regulation, data protection laws, or cybersecurity policy-making; IT and data protection regulators with enforcement experience in data breach investigation and algorithmic

The last sample included 25 participants in the following five professional categories: cyber and data protection lawyers (n = 7), cybersecurity professionals (n = 5), national policymakers (n = 5), data protection and IT regulators (n = 5), and academic legal scholars (n = 3). The participants were geographically spread over jurisdictions such as the European Union (Germany, France, Netherlands), the United Kingdom, the United States, India, Pakistan, and the Gulf Cooperation Council region so that the findings are representative of the regulatory diversity of worldwide AI and data protection regulation, rather than one jurisdiction. Professional legal networks, contacts with regulatory bodies, referral by academic institutions, and targeted recruitment of practitioners with publicly visible experience in relevant areas were also used to conduct recruitment. Thematic saturation was established at the end of the 22 nd interview and three more confirmatory interviews followed.

3.3 Data Collection

Semi-structured, in-depth interviews were used to collect primary data between March and October 2024. This timing was carefully set to capture practitioner views in the immediate post-entry force of the EU AI Act, to offer a contemporary practitioner evaluation of this historic regulatory creation. The interviews took place through encrypted videoconferencing systems, and the average interview sessions lasted 72 minutes. A themed interview guide based on six thematic areas, reflective of the thematic structure that had been identified through analysis, was used to address: (1) the most important current legal issues in AI-driven data processing; (2) the sufficiency of current cyber law frameworks to address AI-enhanced threats; (3) the practical issues of establishing algorithmic accountability

requirements; (4) cross-border jurisdictional issues in AI and data protection The guide was piloted by two legal practitioners and revised to have a proper depth, neutrality, and coverage of the thematic domains of the study.
The secondary data sources included systematic documental analysis of: primary legislative and regulatory instruments such as the EU GDPR and EU AI Act, and the CCPA and PIPL, as well as the India DPDPA, the UK GDPR and Pakistan PECA; leading judicial rulings such as the Schrems I and II CJEU The extensive documentary corpus facilitated the solid triangulation of professional interview results with primary legal authority and institutional analysis.

3.4 Thematic Analysis

The analysis of data was based on the six steps of thematic analysis protocol provided by Braun and Clarke (2006). Initial open coding with NVivo qualitative analysis software came after a lot of familiarization with data by reading all 25 interview transcripts and documentary materials. The process of coding was uniformly used on both interview and documentary data, thus facilitating triangulated theme production which relied on expert narrative analysis as well as primary analysis of legal sources. The codes were then sorted into thematic groups in several rounds of theme development, review and refinement, which eventually results in six major themes having a specific structure of sub-themes. Member checking with 18 of 25 participants, peer debriefing with two academic colleagues in cyber law and AI ethics respectively, and constant comparative analysis to ensure that all primary themes would be evidenced by convergent evidence across data sources and categories of participants all helped to establish theme validity.

3.5 Trustworthiness and Ethics

Reliability was achieved through the triangulation of interview and documentary sources of data, member checking, peer debriefing and maintenance of an elaborate audit trail. Since the sensitivity of some of the disclosures of participants was both political and professional, especially in the context of regulatory enforcement constraints and other organizational compliance failures, specific consideration was given to the protections of confidentiality. The respondents were given coded identifiers of professional classification and all information relating to an organization was eliminated in all analysis records. Data collection came only after the institutional ethical approval was received, all participants signed the written informed consent with clear withdrawal clause, and interviews data were deposited in encrypted institutional repositories that could be accessed by the research team only.

4. ANALYSIS AND FINDINGS

4.1 Introduction: Regulatory Environment in Jurisdictions

It is educative to place the analysis in the context of comparative regulatory environment across the major jurisdictions involved in the study before providing thematic results of the expert interviews. Table 1 offers a comparative overview of the main AI and data protection laws, their enforcement agencies, and penalties in eight jurisdictions, indicative of the regulatory heterogeneity of the world that forms the legal issues and governance solutions at the heart of the research question under consideration. Expert participant perspectives can only be interpreted within this comparative context and the perspectives of experts were bound to be influenced by the particular regulatory environments that participants were placed in.

Table 1. Comparative Global AI & Data Protection Regulatory Frameworks (2024)

Jurisdiction	Key Legislation / Framework	Scope & Coverage	Enforcement Body	Notable Penalty / Provision
European Union	General Data Protection Regulation (GDPR, 2018); EU AI Act (2024)	Comprehensive data rights; AI risk classification (unacceptable/high/limited/minimal)	European Data Protection Board (EDPB); National DPAs	Up to €30M or 6% global turnover; Prohibited AI systems banned outright
United States	California Consumer Privacy Act (CCPA, 2020); Executive Order on AI (2023); NIST AI RMF	Sectoral approach; no federal omnibus data law; federal AI guidance	FTC; State Attorneys General; NIST (advisory)	CCPA: up to $7,500 per intentional violation; FTC enforcement actions
United Kingdom	UK GDPR; Data Protection Act 2018; Online Safety Act (2023); UK AI Regulation White Paper (2023)	Post-Brexit adapted framework; principles-based AI oversight	Information Commissioner's Office (ICO)	Up to £17.5M or 4% global turnover; ICO enforcement notices

China	Personal Information Protection Law (PIPL, 2021); Cybersecurity Law (2017); Generative AI Regulations (2023)	State-centric data sovereignty; mandatory security assessments for cross-border transfers	Cyberspace Administration of China (CAC)	Up to ¥50M or 5% annual revenue; suspension of services; criminal liability
India	Digital Personal Data Protection Act (DPDPA, 2023); IT Act (2000, amended 2008)	Consent-based data processing; data fiduciary obligations; significant data fiduciary regime	Data Protection Board of India (DPBI – to be established)	Up to ₹250 crore per violation; sector-specific penalties
Brazil	Lei Geral de Proteção de Dados (LGPD, 2020)	GDPR-influenced; 10 legal bases for processing; data subject rights	Autoridade Nacional de Proteção de Dados (ANPD)	Up to 2% of Brazilian revenue capped at R$50M per violation
Pakistan	Prevention of Electronic Crimes Act (PECA, 2016); Personal Data Protection Bill (Draft, 2023)	Cybercrime provisions; draft data protection framework pending enactment	FIA Cybercrime Wing; Proposed National Commission for Personal Data Protection	PECA: up to 3 years imprisonment; fines up to PKR 10M

Note. Legislative and regulatory information reflects the status of frameworks as of October 2024. Penalty provisions represent maximum theoretical exposure and do not reflect typical enforcement outcomes. GDPR enforcement data sourced from the EDPB's enforcement tracker (2024). Abbreviations: DPA = Data Protection Authority; FTC = Federal Trade Commission; NIST = National Institute of Standards and Technology; CAC = Cyberspace Administration of China; ICO = Information Commissioner's Office; FIA = Federal Investigation Agency.

Comparative regulatory scene as shown in Table 1 displays some analytically important patterns which give a critical background to the perceptions of expert participants. First, the EU is uniquely regulatory, both the GDPR and the EU AI Act present a regulatory framework of substantial ambition and seriousness of enforcement that no other jurisdiction fully emulates - a regulatory asymmetry that creates the Brussels Effect of global standard-setting effect, and creates a high compliance burden on global technology companies. Second, the reliance on sectoral and state level approaches that remain in place in the United States without federal omnibus data privacy or AI legislation results in a spotty compliance landscape that professional actors have consistently described as ineffective when it comes to the systemic demands of AI-driven data processing. Third, the unique data governance model of China, based on extensive data subject rights, robust state access privileges, and strict cross-border transfer controls raises inherent incompatibility strains with the adequacy requirements of GDPR that have not yet been addressed in a bilateral regulatory dialogue. Fourth, the emerging world regulatory landscape - such as India and Pakistan - demonstrates not only a real advancement in data protection law-making but a serious lack of implementation and enforcement capacity that makes formal legislative structures much less effective in practice than they appear on paper.

Direct questions were posed to expert participants to determine how well their jurisdictions regulate the legal issues presented by AI systems. The answers were nearly evenly critical in the jurisdictional settings, but the nature of inadequacy was quite varied. Implementation complexity and a lack of enforcement capacity were cited by EU-based participants as the main adequacy concern; structural insufficiency of the sectoral approach to addressing AI-specific systemic risks by U.S. participants; enforcement institutional capacity and the lack of rule of law by South Asian participants; and all practitioners across jurisdictions agreed on the inadequacy of any single national framework to regulate AI systems the training, deployment, and impact

4.2 Theme 1: AI Systems and Privacy and Data Rights

The most widely reported legal issue among all categories of participants was privacy violations linked to AI-based data processing, which demonstrates the inherent contradiction between the insatiable demand of AI systems to process large amounts of personal data and the legal frameworks of consent-based data processing that were created to regulate personal data processing in a more limited and intentional context. Data protection lawyers were especially thorough in their descriptions of the discrete consent architecture issues that AI systems create that uses personal data in a manner that was not and often could not have been envisaged at the time of initial consent.

The idea of the purpose limitation, i.e. the GDPR principle that states that personal data must be collected with specified, explicit and legitimate purposes and that must not be further processed in a way that would be inconsistent with the purposes, was pointed out by several participants in the legal expert group as the most structurally problematic concept of data protection within the context of the development and deployment of AI systems. The datasets used to train large language models and other foundation AI models are a combination of various sources over a long period of time, and their purpose may be completely unspecified or not fully defined at the time of data collection. The ex-post facto transfer of personal data, which was initially gathered in distinct defined contexts, such as customer service interactions, medical consultations, educational assessment, into AI training data without additional consent, is a systematic contravention of the principle of purpose limitation that is not sufficiently tackled in the existing enforcement frameworks, as practitioners describe it.

AI systems processing biometric data, including facial recognition, voice recognition, gait analysis, and emotion detection, was of particular legal concern to participants in the field, as this type of data is highly sensitive in practically any data protection regime and because massive biometric surveillance by AI significantly imbalances the risks to the personal privacy and autonomy of individuals. The regulatory challenge of real-time biometrics identification systems that the EU AI Act categorically forbids the use of law enforcement in public spaces, with limited exceptions, was described by the participants of the regulator in terms that indicated the practical enforcement difficulties of detecting and penalizing covert biometric data capture in the retail, transport, and public space setting where commercial facial recognition use is not publicly announced.

Practitioners proposed that data minimization, or the idea that the amount of personal data gathered and used must be as minimal as possible to meet certain aims, has structural challenges in AI settings, where model performance tends to be improved with more data, and person-organizational incentives to gather more data than minimization principles permit. Several legal practitioner respondents recounted experiences of client advisory work where they had advised data minimization procedures, which were formally but avoided in practice, such as so-called anonymization methods which were provably reversible in practice in light of the re-identification abilities of current AI systems. The fact that traditional anonymization is not sufficiently a data protection method in the age of AI-driven re-identification has implications of interest to the compliance strategies of data protection based on anonymization as a method of data removal out of legal protection systems.

4.3 Theme 2:Algorithmic Acountabality and Trasnsparency Challanges

The second big thematic area was algorithmic accountability and transparency, which produced the most technically refined participant accounts when legal practitioners, regulators, and cybersecurity experts tackled the problem of how to apply legal accountability frameworks that are designed to apply human decision-making models to systems whose decision-making mechanisms are of an entirely different nature than the model of human deliberation. The fundamental legal dilemma of algorithmic accountability, namely to offer humans meaningful control over automated decision-making processes that impact legal rights and interests when such decisions are made by systems the inner workings of which remain unknown even to their creators, was described by participants as the unresolved issue of the current AI law.

Article 22 of GDPR, the right to explanation, which obliges data controllers to inform the data subject with meaningful information on the logic used in automated decision-making, was greatly discussed by participants with legal expertise whose assessments were largely negative due to the lack of clarity of the contemporary deep learning systems. One practitioner observation that was repeated was the difference between technical explainability which might be possible in some AI architectures using methods such as LIME, SHAP, or attention visualization and legally meaningful explainability which must be understandable to non-technical users, and sufficiently detailed to demonstrate potential discriminatory impact. Participants who were legal experts have always observed that technically generated feature importance explanations would fail to meet either of these legal criteria, and that the disjunction between what AI systems would technically explain and what the legal accountability frameworks would legislatively demand is a core unresolved tension in the present AI governance.

The responses of regulator actors were especially insightful in describing the realities of the enforcement of the algorithmic accountability. Some of the narratives of investigation experiences where algorithmic discrimination complaints had been raised (employment screening, credit assessment, or benefits eligibility determination) had been extremely challenging to investigate due to the inability or unwillingness of the AI system developers to offer the technical documentation needed to determine whether discrimination occurred. The fact that the systems of commercial AI are opaque to regulatory scrutiny and made more so by the intellectual property protection assertions that organizations invoke to fight the release of model architecture and training data information was noted as a basic barrier to effective algorithmic accountability enforcement that is not well addressed by current legal frameworks.

The conformity assessment provisions of the EU AI Act of high-risk AI systems, such as compulsory technical documentation, logging, transparency, human oversight, and accuracy provisions, were evaluated by participants as meaningful steps to achieve algorithmic accountability, but massive reservations were expressed about implementation quality. Experienced legal professionals who advise organizations on compliance with the AI Act have outlined the conformity assessment process as a resource-consuming and possibly creating compliance theater,

the illusion of accountability compliance but not compliance, especially in organizations where commercial pressures to implement AI systems outweigh a careful approach to pre-deployment risk assessment and documentation.

4.4 Theme 3: Cybersecurity, Data Breach Liability, and AI-Enhanced Threats

The cybersecurity aspect of AI legal issues produced a convergent worry among cybersecurity professional and legal practitioner respondents, who generally described the interplay between AI-enhanced offensive cyber capabilities and the current cybersecurity legal frameworks as creating a structural insufficiency of escalating magnitude. The qualitative shift in the nature of cyber threats that AI enabled, between labor-intensive, manually operated, but limited scale, and automated, AI-optimized but larger, more sophisticated, and targeted, was repeatedly cited to pose a legal challenge that did not exist in legal cybersecurity liability frameworks.

AI-generated phishing and social engineering attacks gained widespread attention among cybersecurity professional participants, who described the behavioral sophistication of AI-generated malicious messages, personalized to individual targets based on scraped social media and professional data, and reinforced through reinforcement learning to be as effective as capturing credentials as possible, as a qualitative leap in the previous generation of phishing attacks, and a fundamental threat to the operation of user-education-based cybersecurity The juridicative implications of this increase are considerable: the organizational cybersecurity negligence standards, developed when phishing emails were grammatically unsophisticated, and the attacks were clearly suspected, are already becoming under more doubt when the same organizational defenses fail to stop AI-optimized social engineering attacks of human-surpassing quality.

The Article 33 of GDPR, which stipulates that the data breach must be notified to the supervisory authorities within 72 hours of its discovery, was evaluated by both the legal practitioner and regulator participants as more and more incongruent with the realities of AI-enhanced data breach situations. The participants of the cybersecurity profession outlined scenarios of multi-stage attack AI-based autonomous reconnaissance, vulnerability identification and exploitation, data extraction, cover-up over the course of weeks or months, which do not become detectable until weeks or months after the initial breach incident, and makes the 72-hour notice period practically irrelevant in most advanced attack cases. Some regulators have admitted the practical challenges of implementing notification deadlines against those organizations who cannot in fact identify any breaches within the given time frame because of the stealthiness of AI-enhanced attackers.

4.5 Theme 4: Legal Loopholes and Jurisdiction Problems in Global AI Governance

The fourth thematic area was legal gaps and jurisdictional issues in global AI regulation, which produced the most policy-oriented participant accounts of participants in the policymaker and international regulatory practitioner groups that work everyday at the boundaries between existing national regulatory systems. The basic jurisdictional challenge of AI governance that AI systems are created, trained, launched, and influence a variety of national jurisdictions at the same time, but legal frameworks are still largely national in their jurisdictional focus and limited in their extraterritorial reach has been continually cited as the structurally most challenging problem in the international AI governance landscape.

The strategic organization of AI creation and deployment to seek advantages amid country regulatory differences — regulatory arbitrage was recognized by policymaker respondents as an increasingly important issue of governance. Some of the participants detailed particular practices such as routing AI training computation to jurisdictions with few AI governance responsibilities, localizing the process of data processing to jurisdictions with lax enforcement of data protection regimes and offering services to users in high-regulation jurisdictions, and carving out corporate entities in a way that enables taking advantage of interpretive ambiguities in the territorial coverage of laws such as the GDPR and the EU AI Act There are systematic limitations on the practical application of extraterritorial regulatory claims against foreign actors, especially against those found in jurisdictions with weaker traditions of regulatory cooperation, which provide systematic gaps in the governance that can be used by sophisticated actors.

The jurisdictional conflict between the cross-border data transfer requirements of GDPR and the data localization and government access requirements of the Data Security Law in China is the most commercially important current jurisdictional conflict in the global data governance arena. The compliance requirements of multinational corporations in EU and Chinese jurisdictions are truly irreconcilable: the standard contractual clause of GDPR on cross-border transfers cannot be met in a way that would both meet the criteria of state access and localization of the Chinese jurisdiction, and there is no adequacy decision between the EU and China. Participants involved in policymaking and legal practice characterized this conflict as giving rise to routine compliance impossibilities that organizations cope with by compartmentalization, strategic ambiguity, and jurisdictional arbitrage instead of by effective simultaneous compliance - a state of affair that constitutes a serious governance failure in the practical protection of individual data subjects.

4.6 Theme 5: New Regulatory Reactions and the EU AI Act

The most prospective and prescriptive accounts of participants in the AI case studies were new regulatory reactions to the legal issues posed by AI, with policymakers, regulators, and legal practitioners detailing their evaluations of existing regulatory efforts and their suggestions on how to develop governance. EU AI Act was the topic of discussion

most often with regard to new regulatory responses, which is understandable given that it is the most substantive and globally important piece of legislation on AI regulation to date at the time when the study was collecting data.
A detailed thematic results summary is provided in table 2 based on the analysis of all six main themes, combining expert interview data with documentary data to give a summarised account of the analytical results of the study within the entire thematic range.

Table 2. Thematic Analysis — Key Themes, Sub-Themes, and Expert Insights (n = 25)

Theme	Sub-Themes	Key Expert Insights & Findings
Privacy & Data Rights in AI Systems	Biometric surveillance; profiling; data minimization violations; consent architecture failures	Participants confirmed that AI systems processing biometric and behavioral data routinely operate beyond the scope of original consent, with 18 of 25 experts identifying consent architecture design as the most critical unresolved legal challenge in AI-driven data processing. Automated profiling was identified as creating legally cognizable harm in employment, credit, and criminal justice contexts where algorithmic outputs substitute for human deliberation without adequate transparency.
Algorithmic Accountability & Transparency	Explainability obligations; black-box systems; right to explanation; audit requirements	Legal expert and regulator participants converged on explainability as the central jurisprudential challenge of AI governance: courts and regulatory bodies cannot assess whether algorithmic decisions violate legal norms they cannot understand. The EU AI Act's Article 13 transparency requirements were identified as the most substantive current regulatory response, though participants cautioned that technical explainability does not automatically translate into legally meaningful explanations accessible to affected individuals or non-specialist adjudicators.
Cybersecurity & Data Breach Liability	Breach notification obligations; attribution challenges; state-sponsored attacks; AI-enhanced threats	Cybersecurity professional participants highlighted a systematic underestimation of AI-enhanced attack sophistication in existing cyber law frameworks. AI-generated phishing, deepfake social engineering, and automated vulnerability exploitation were identified as creating qualitative escalations in cyber threat severity that existing breach notification and liability frameworks — designed around human-operated attacks — inadequately address. Attribution of AI-enhanced attacks across jurisdictional boundaries was characterized as approaching impossibility under current legal frameworks.
Legal Gaps & Jurisdictional Conflicts	Cross-border data flows; regulatory arbitrage; conflicting national standards; enforcement gaps	Policymaker participants identified regulatory fragmentation as the most operationally significant challenge in global AI and data protection governance. The conflict between the EU's extraterritorial GDPR reach, China's data localization requirements, and the United States' sectoral approach creates systematic compliance impossibilities for multinational technology organizations and produces regulatory arbitrage opportunities that enable governance evasion through strategic data routing and corporate structuring.
Emerging Regulatory Responses to AI	EU AI Act implementation; national AI strategies; sandboxes; co-regulatory models	Regulator and legal expert participants expressed cautious optimism regarding the EU AI Act as a global regulatory benchmark, while noting significant implementation uncertainty regarding technical standard development, conformity assessment body designation, and enforcement coordination across member states. AI regulatory sandboxes — enabling controlled testing of AI systems under regulatory supervision — were identified

		as the most practically promising mechanism for managing innovation-risk tradeoffs in rapidly evolving AI application domains.
Generative AI & Intellectual Property	Copyright in AI outputs; training data legality; liability for AI-generated harmful content; deepfakes	The generative AI intellectual property dimension generated the most divergent expert perspectives, reflecting genuine unresolved doctrinal uncertainty across jurisdictions. Participants with copyright law expertise noted that existing copyright frameworks — built around human authorship — provide inadequate and inconsistent guidance for AI-generated output ownership, with current court decisions in the United States, United Kingdom, and EU pointing in divergent directions that create commercial uncertainty for generative AI product developers and deployers.

Note. Thematic findings derived from systematic thematic analysis of 25 expert semi-structured interviews and corroborated through documentary analysis of primary legal sources. Sub-theme descriptions and key insights represent synthesized cross-participant perspectives rather than verbatim participant quotations. All participant contributions are anonymized using professional category codes throughout the analysis.

Assessments of the EU AI Act by participants indicated overall agreement that the EU AI Act is a significant and historic regulatory step and indicated a lot of concern about the quality of implementation and enforcement capacity and speed of development of technical standards compared to compliance deadlines of the Act. Lawyers representing multinational technology companies explained their compliance planning issues in language that emphasized the significant interpretive ambiguity that still existed in the interpretation of the Act as applied to particular types of AI systems, implementation situations, and situations involving cross-border operations. The six-month, twelve-month, and twenty-four-month staged implementation plan, where, as of February 2025, the prohibited practices would become enforceable, and in August 2026, the high-risk system requirements would, where applicable, become enforceable, was described by some participants as a compliance planning cliff to organizations that had not prepared to address the AI Act by the time the Act gained formal effect.Regulator and policymaker participants identified AI regulatory sandboxes as the most feasibly promising type of governance innovation currently underway, wherein organizations can experiment with AI systems under regulatory oversight and in controlled operational settings. Regulatory sandboxes in every member state are required by the EU AI Act, and participants cited early examples in Spain (the AESIA sandbox), the United Kingdom (ICO and FCA sandboxes) and Singapore (the MAS regulatory sandbox) as offering valuable experience of what it takes to develop an effective AI regulatory supervision framework. A number of participants pointed to the fact that properly designed sandboxes would be capable of both facilitating regulatory capacity building - by offering direct experience with state-of-the-art AI systems - and mitigating the threat of innovation stifling of ex ante regulation by offering a controlled testing environment to new AI applications before they are required to meet all compliance standards.

4.7Theme Generative AI ,Intellectuall Property ,and New Legal Fronitiers

The generative AI aspect of the research - including large language models, image creation systems, synthetic media, and multimodal AI - produced some of the most thought-provoking participant descriptions, as legal professionals and academic academics tackled legal issues that are truly novel and whose solution using the current legal systems is highly disputed. The speed of commercial, creative and professional use of generative AI has created legal issues in the areas of intellectual property, defamation, consumer protection and professional liability, only recently being tackled by legislative and judicial systems.

The legal status of the intellectual property of generative AI training, in particular, whether the mass reproduction of copyrighted material in AI training datasets amounts to copyright infringement under the relevant national law, is actively being contested in various jurisdictions with possibly different results. Authors, visual artists, and news publishers have brought several class action lawsuits against the largest AI developers such as OpenAI, Stability AI, and Anthropic, with the overall legal question being whether the temporary reproducing of copyrighted works during the training process, as well as the output of works that can reproduce recognizable aspects of training works, is covered or is not covered by the doctrine of fair use. Participants who are experts in the law and have a specialization in copyright provided varied determinations of probable outcomes, which indicate a real doctrinal ambiguity that will ultimately need a legislative solution or official Supreme Court interpretation.

Deepfake technology, AI-synthetic media that convincingly represent actual individuals saying or doing things that they did not say or do, was singled out by participants in categories as causing the most acute and immediate harm-inducing uses of generative AI, including non-consensual intimate imagery, political disinformation, identity fraud, and reputational attacks with potentially catastrophic individual and social outcomes. The legal system of deepfake regulation is still highly fragmented: a number of U.S. states have developed deepfake-specific legislation, such as electoral manipulation and non-consent intimate imagery, the Online Safety Act in the United Kingdom introduces

platform responsibility to remove deepfake non-consent intimate imagery, and deep synthesis regulations in China provide content labeling requirements to synthetic media creators - but there is not yet a global deepfake govern

5. DISCUSSION

The results of this paper shed light on a legal and regulatory framework across the world that is literally failing to match the pace, magnitude and newness of the legal issues of AI - and whose structural weakness is not an incidental failure that can be addressed through minor legislative changes but a structural problem that represents a conflict between the architectural design of our legal systems and the nature of AI technology. There are three structural tensions that are especially analytically important.

To begin with, the consent structure of modern data protection legislation, which is constructed on the basis of the assumption that people are able to give meaningful, informed and voluntary consent to limited, bounded uses of their personal data, is simply incompatible with the logic of operation of AI systems that make their value precisely in aggregating, repurposing and discovering new patterns in large collections of personal data that no single consent specification could reasonably anticipate. Not merely an issue of implementation quality or regulatory enforcement energy but a structural incompatibility between the design of legal frameworks and the technological actuality that needs some foundational reconceptualization of the governance of data protection and not a policy of enforcement improvement. The other models under consideration, collective licensing models, public interest exceptions to AI training, data trusts and commons, are promising approaches but still must be developed considerably further before they can offer practical alternatives to the currently broken consent architecture to AI settings.

Second, the jurisdictional structure of the modern international law, based on the territorial sovereignty and the effective ability of the state to control the behavior within its borders, is becoming less and less sufficient to control AI systems whose creation, education, implementation, and outreach routinely and simultaneously affect dozens of jurisdictions with different legal demands. The practical regulatory arbitrage possibilities arising due to this jurisdictional fragmentation compromise even the most ambitious national regulatory efforts, as seen in the continued clash between EU GDPR-based requirements and Chinese PIPL as well as data localization requirements. Effectual AI governance ultimately entails multilateral institutional structures - in the fashion of multilateral regimes in international trade, aviation safety, or nuclear technology - which are still completely lacking in the global AI governance environment, although there is early multilateral consultation, in terms of G7, G20, OECD and UN.

Third, the reactive temporal organization of legal systems, which generally reacts to documented harms by means of retrospective rule-making and adjudication, is insufficient to regulate AI technologies whose greatest dangers might arise at systemic scales and speeds that swamp retrospective regulatory actions. The risks to financial stability of AI-based high-frequency trading, the risk of democratizing AI-generated electoral disinformation, and the risks of AI systems in critical infrastructure necessitate anticipatory governance measures, such as compulsory pre-deployment assessment of risks, regulatory sandbox, algorithmic audit requirements, and AI incident reporting systems, that create early warnings of emergent risks before they become harms at scales that can be effectively dealt with through ret

6. CONCLUSION AND RECOMMENDATIONS

This paper has presented an empirically based, in-depth analysis of the legal issues and regulatory action at the cross-roads of artificial intelligence, cyber law, and data protection in 2024. Using the experience of 25 well-selected key informants in legal practice, regulatory regulation, cybersecurity, and policy spheres, with additional support of systematic documentary analysis of primary legal materials in major world legal systems, the study has identified six thematic areas of AI-related legal challenge, including privacy and data rights, algorithmic accountability, cybersecurity and breach liability, regulatory reactions, and the new legal frontiers of generative AI, whose cumulative weight

The analysis implies five policy recommendations. To start with, risk-based AI regulatory frameworks in jurisdictions that lack extensive regulation of AI in particular, specifically in the United States on federal level, should be enacted by the legislative bodies that would regulate the unique legal issues associated with automated decision-making, training data management, and AI-enhanced cybersecurity risks beyond the scope of the current regulatory frameworks. Though there are challenges in implementing the EU AI Act, it offers a substantive framework whose fundamental risk-tiering framework is a suitable basis on which countries should adapt it. Second, international governance institutions, especially the United Nations, OECD and G20, need to immediately focus on the creation of multilateral AI regulation systems that would resolve jurisdictional disputes, regulatory arbitrage, and coordination of enforcement needs that cannot be fulfilled in a single country by any country regulatory system. The report by the UN High-Level Advisory Body on AI (2024) is a valuable piece of background analysis, but needs to be transformed into a binding set of multilateral commitments, not a set of voluntary principles. Third, data protection regulators are required to significantly expand both technical capability of algorithmic audit and investigation, and machine learning skills, legal discovery authority, and AI training data law enforcement liaison mechanisms required to efficiently

investigate and penalize algorithmic discrimination, privacy infringement and AI training data lawfulness violations. Fourth, legal compliance assessment should be a built-in element in the governance of the AI systems development lifecycle, i.e., at the beginning of data sourcing, model development, testing, deployment, and monitoring, instead of viewing compliance as an audit process after the fact. Fifth, law enforcement of intellectual property and deepfake issues of generative AI should be hastened in every jurisdiction, where the emphasis should be on setting up clear legal foundations in the use of AI training data, the mandatory stipulation of synthetic media labels, and the development of strong remedies to victims of offensive deepfake images.

Limitations of this study must be mentioned. The qualitative design offers depth of analysis and practitioner foundation but lacks statistical generalizability. Although the sample is well designed to capture the breadth of the expertise, it may not be representative of the full range of legal and regulatory views in 160+ jurisdictions with data protection systems. Owing to the fast changing nature of the subject matter, some of the findings may need a revision as the regulatory implementation advances and judicial case law becomes established. Future studies must combine qualitative practitioner insights with quantitative regulatory compliance and enforcement outcome measures to give a more comprehensive view of AI law operational efficiency - how well legal frameworks on paper are reflected in real AI systems governance.

The acuity of the governance issues that are detected in the present study cannot be overestimated. Artificial intelligence is not a technology of the future, whose legal consequences can be postponed to a later time when the legal frameworks have been developed, but a current and fast-growing technology that already causes legal harms at large-scale levels in all the largest jurisdictions. The regulatory ambition, institutional capacity building, inter-country coordination and organizational commitment of compliance that effective AI governance necessitates demand both urgent and enduring action on the part of all interested parties. The expenses of the current governance inefficiency, namely, in terms of the violations of individual rights, undermining the democratic integrity, harm to cybersecurity, and the risk in the functioning of the economic system, are significantly higher than the expenses of proactive and properly designed regulation investment.

REFERENCES

1. Barocas, S., Hardt, M., & Narayanan, A. (2019). Fairness and machine learning: Limitations and opportunities. MIT Press. https://fairmlbook.org
2. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa
3. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Héigeartaigh, S. Ó., Beard, S., Riedl, M., Jayber, W., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv:1802.07228. https://arxiv.org/abs/1802.07228
4. Calo, R. (2017). Artificial intelligence policy: A primer and roadmap. UC Davis Law Review, 51(2), 399–435.
5. Council of Europe. (2001). Convention on cybercrime (ETS No. 185). Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
6. Denzin, N. K., & Lincoln, Y. S. (2018). The SAGE handbook of qualitative research (5th ed.). SAGE Publications.
7. Doshi-Velez, F., Kortz, M., Budish, R., Bavitz, C., Gershman, S., O'Brien, D., Scott, K., Schieber, S., Waldo, J., Weinberger, D., Wood, A., & Wood, W. (2017). Accountability of AI under the law: The role of explanation. Berkman Klein Center Working Paper. https://doi.org/10.2139/ssrn.3064761
8. European Data Protection Board. (2024). GDPR enforcement tracker: Annual statistics report 2023. EDPB. https://www.edpb.europa.eu
9. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People — An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
10. Information Commissioner's Office. (2023). Guidance on AI and data protection. ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/
11. Kuner, C. (2020). The Court of Justice of the EU judgment in the Schrems II case: A brief analysis. International Data Privacy Law, 10(4), 280–285. https://doi.org/10.1093/idpl/ipaa020
12. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21. https://doi.org/10.1177/2053951716679679
13. NIST. (2023). Artificial intelligence risk management framework (AI RMF 1.0). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1
14. OECD. (2024). OECD AI policy observatory: Global overview of AI policy and governance developments 2024. OECD Publishing. https://oecd.ai

15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). (2016). Official Journal of the European Union, L 119, 1–88.
16. 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). (2024). Official Journal of the European Union, L, 2024/1689.
17. Schwartz, P. M., & Solove, D. J. (2014). Reconciling personal information in the United States and European Union. California Law Review, 102(4), 877–916.
18. Solove, D. J., & Hartzog, W. (2022). Breached! Why data security law fails and how to improve it. Oxford University Press.
19. Statista Research Department. (2024). Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2025. Statista. https://www.statista.com/statistics/871513/worldwide-data-created/
20. Taddeo, M., & Floridi, L. (2018). The debate on the moral responsibilities of online service providers. Science and Engineering Ethics, 22(6), 1575–1603. https://doi.org/10.1007/s11948-015-9734-1
21. UNCTAD. (2024). Data protection and privacy legislation worldwide. United Nations Conference on Trade and Development. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
22. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer. https://doi.org/10.1007/978-3-319-57959-7
23. Wachter, S., Mittelstadt, B., & Russell, C. (2017). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 841–887.
24. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.