

Artificial Intelligence, Data Science and Automation: An Integrated Framework for Responsible Adoption, Data Governance and Workforce Upskilling, with Comparative Evidence from Nigeria

Nwankwe, Dimie^{1*}, Boye Aziboledia Frederick² and V.I.E Anireh³

^{1,3}Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

²Federal University Otuoke, Bayelsa State, Nigeria.

*Corresponding Author

Nwankwe, Dimie

Email:

dimie.nwankwe@gmail.com

Co-author emails:

boyeaf@fuotuoike.edu.ng;

anireh.ike@ust.edu.ng

Article History

Received: 19.08.2026

Revised: 11.09.2026

Accepted: 02.10.2026

Published: 21.10.2026

Abstract: Artificial Intelligence (AI), Data Science and Automation are transforming organisations, labour markets and public administration, yet their adoption raises interrelated concerns about ethics, data governance, privacy, cybersecurity and workforce displacement. This paper examines these dimensions together and proposes a framework for responsible, human-centered AI-driven automation, with particular attention to Nigeria. The study combines an integrative review of multidisciplinary literature with qualitative document analysis of legal and policy instruments and a comparative analysis of documented cases across ten jurisdictions: Nigeria, Ghana, Kenya, Rwanda, the United States, the United Kingdom, Spain, France, Germany and China. AI principles have converged internationally but remain difficult to operationalise; data governance is the foundation on which fairness, privacy and security depend; AI introduces distinctive attack surfaces such as data poisoning, model extraction and membership inference; and automation transforms tasks more often than it eliminates whole occupations, making upskilling decisive. Nigeria exhibits rapid deployment of data-intensive systems alongside a governance lag, although regulatory enforcement under the Nigeria Data Protection Act 2023 is strengthening. The paper proposes the Integrated Responsible Automation Framework (IRAF), which positions data governance as the foundation for three pillars (responsible and ethical AI, privacy and security by design, and workforce and organisational readiness), maps controls to the AI lifecycle, and derives four testable propositions. It offers actionable guidance for policymakers, organisations and educators, especially in emerging economies.

Keywords: artificial intelligence; data science; responsible AI; AI ethics; data governance; data privacy; cybersecurity; intelligent automation; future of work; upskilling; Nigeria.

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/) (CC BY-NC 4.0)

Cite this article:

Nwankwe, N., Frederick, B. A., and Anireh, V. I. E., (2026). Artificial Intelligence, Data Science and Automation: An Integrated Framework for Responsible Adoption, Data Governance and Workforce Upskilling, with Comparative Evidence from Nigeria. *ISAR Journal of Science and Technology*, 4(10), 40-62.

1. INTRODUCTION

Artificial Intelligence (AI), Data Science and Automation are reshaping industries, public administration and society at an unprecedented pace. Organisational adoption of AI has expanded markedly: McKinsey's global surveys report that the share of respondents whose organisations had adopted AI in at least one business area more than doubled between 2017 and 2022, from 20 per cent to 50 per cent (Chui et al., 2022), and that by early 2025, 78 per cent of respondents reported AI use in at least one business function (Singla et al., 2025). These technologies allow organisations to process large volumes of data, automate complex workflows and support decisions in healthcare, finance, logistics, energy, education and government (Dwivedi et al., 2021; Jordan & Mitchell, 2015). Advances in machine learning, deep learning, big-data analytics and robotic process automation (RPA) have further accelerated digital transformation in both the public and private sectors (LeCun et al., 2015; van der Aalst et al., 2018).

However, as Brynjolfsson and McAfee (2014) caution, technological progress frequently outpaces the adaptation of institutions, skills and social protections, creating new forms of inequality and uncertainty. The International Monetary Fund estimates that almost 40 per cent of global employment is exposed to AI, with advanced economies more exposed but also better positioned than emerging and developing economies to capture its benefits (Cazzaniga et al., 2024). The convergence of AI, Data Science and Automation therefore represents not only a technological shift but also a socio-economic and governance transformation. Alongside these opportunities, AI-driven systems introduce significant ethical, legal and organisational risks. Algorithmic bias, opaque decision-making, misuse of personal data, privacy violations and new cybersecurity vulnerabilities have become prominent concerns for researchers, regulators and the public (Mittelstadt et al., 2016; Barocas & Selbst, 2016). Documented cases, including a commercial healthcare algorithm that systematically under-estimated the needs of Black patients (Obermeyer et al., 2019) and a welfare-fraud risk system struck down by a Dutch court (van Bekkum & Zuiderveen Borgesius, 2021), demonstrate that these risks are not hypothetical. As AI increasingly informs high-stakes decisions in credit, recruitment, medicine, policing and public services, the demand for responsible and accountable AI governance has become pressing (Floridi et al., 2018; Jobin et al., 2019).

Furthermore, the trustworthiness of AI is inseparable from the quality, governance and security of the data on which it depends (Janssen et al., 2020). Weak data governance undermines system reliability, exposes organisations to regulatory sanctions and amplifies privacy and cybersecurity risk. At the same time, intelligent automation is

restructuring tasks, occupations and skill requirements: some tasks are displaced, others are transformed and new ones are created, which requires large-scale reskilling and upskilling (Acemoglu & Restrepo, 2019; World Economic Forum [WEF], 2025).

Although each of these themes has a substantial literature, they are usually examined in isolation: AI ethics scholarship rarely engages with workforce transition, labour-economics research seldom addresses data governance, and governance research is concentrated on North American and European jurisdictions (Birhane, 2020; Gwagwa et al., 2020). Evidence from African contexts, where AI deployment frequently runs ahead of regulatory and institutional capacity, remains comparatively limited (Eke et al., 2023). This paper addresses that gap by integrating these domains and grounding the analysis in comparative evidence from Nigeria and nine other jurisdictions.

1.1 Objectives and research questions

The aim of this paper is to provide an integrated examination of the ethical, governance, security and workforce implications of AI, Data Science and Automation, and to propose a framework for their adoption responsible. Specifically, the study addresses the following research questions (RQs):

- **RQ1:** What principles and practices constitute responsible and ethical AI, and how are they operationalised across the AI lifecycle?
- **RQ2:** How do data governance, privacy and cybersecurity interact as foundations for trustworthy AI, and how do governance arrangements differ between Nigeria and comparator jurisdictions?
- **RQ3:** What are the employment and organisational impacts of AI-driven automation, and which upskilling and reskilling strategies are required?
- **RQ4:** How can these dimensions be integrated into a coherent framework that supports sustainable, human-centered AI-driven automation, particularly in emerging economies such as Nigeria?

1.2 Contributions

The paper makes three contributions. First, it synthesises multidisciplinary literature on AI ethics, data governance, privacy, AI-specific cybersecurity and the future of work, which are usually treated separately. Second, it provides a structured comparative analysis of AI-relevant governance and workforce instruments in Nigeria, Ghana, Kenya, Rwanda, the United States, the United Kingdom, Spain, France, Germany and China, supported by verifiable statutory and enforcement evidence. Third, it proposes an Integrated Responsible Automation Framework (IRAF) that positions data governance as the foundation for three mutually reinforcing pillars (responsible AI, privacy and

security by design, and workforce readiness) and derives testable propositions for future empirical research.

The remainder of the paper is organised as follows. Section 2 describes the research methodology. Section 3 establishes conceptual foundations. Sections 4, 5 and 6 examine responsible AI; data governance, privacy and cybersecurity; and automation, the future of work and upskilling, respectively. Section 7 presents the integrated framework, Section 8 discusses implications and limitations, and Section 9 concludes.

2. RESEARCH METHODOLOGY

The study adopts an integrative literature review design, which is appropriate where the objective is to synthesise mature but fragmented bodies of knowledge and generate new conceptual frameworks rather than to aggregate effect sizes (Torraco, 2005; Snyder, 2019). This design was complemented by qualitative document analysis of legal and policy instruments (Bowen, 2009) and by a comparative case analysis of documented AI and data-governance incidents.

Sources. Three categories of source were used: (i) peer-reviewed journal articles and conference proceedings in computer science, information systems, law, ethics and labour economics; (ii) authoritative books and standards, including ISO/IEC standards and the NIST AI Risk Management Framework; and (iii) primary legal and policy documents (statutes, regulations, national strategies and regulator decisions) together with reputable reports of enforcement actions. Preference was given to highly cited foundational works and to recent studies (2019–2026) reflecting developments such as generative AI and the EU Artificial Intelligence Act.

Selection of jurisdictions. Nigeria is the focal case. Comparator jurisdictions were selected purposively to represent (a) other African approaches at different stages of maturity (Ghana, Kenya and Rwanda); (b) the rights-based European model (Spain, France and Germany, all subject to the GDPR and the EU AI Act) and the United Kingdom's post-Brexit variant; (c) the sectoral, market-led model of the United States; and (d) the state-centric model of China.

Verification. Every bibliographic reference was checked against its publisher record or Digital Object Identifier (DOI), and every legal instrument and enforcement action against an official source or a reputable news outlet. Claims that could not be independently verified were removed. Comparative judgements of governance maturity presented in Section 5 are the authors' qualitative synthesis of the documented evidence and are identified as such.

3. CONCEPTUAL FOUNDATIONS

3.1 Artificial Intelligence

Artificial Intelligence refers to computational systems designed to perform tasks that ordinarily require human intelligence, including perception, learning, reasoning, problem-solving and decision-making (Russell & Norvig, 2021; Kaplan & Haenlein, 2019). Contemporary AI is predominantly data driven machine learning and deep learning models learn statistical patterns from large datasets to generate predictions, classifications and content that support automated or semi-automated decisions (Jordan & Mitchell, 2015; LeCun et al., 2015). Also, the challenges of implementing AI-based cybersecurity, including ethical concerns, data privacy, and the risk of adversarial AI attacks (Boye et al, 2024) added the necessity for a fair approach to harness AI's potential while ensuring robust, secure, and efficient energy operations.

3.2 Data Science

Data Science is an interdisciplinary field that integrates statistics, computer science and domain expertise to extract actionable knowledge from structured and unstructured data (Provost & Fawcett, 2013; Dhar, 2013). It supplies the methodological pipeline on which AI depends data collection, preparation, exploratory analysis, modelling, evaluation and deployment (Cao, 2017; Donoho, 2017). Consequently, weaknesses at any stage of the data pipeline propagate directly into the behaviour of AI systems.

3.3 Automation and Intelligent Automation

Automation is the execution by a machine of functions previously carried out by humans, and it can be implemented at varying levels across information acquisition, analysis, decision selection and action implementation (Parasuraman et al., 2000). Traditional automation, including RPA, relies on predefined rules and structured workflows (van der Aalst et al., 2018; Willcocks et al., 2017). When combined with machine learning, natural language processing and analytics, it becomes intelligent automation, able to handle semi-structured and unstructured inputs, adapt to changing conditions and continuously optimise processes (Syed et al., 2020; McAfee & Brynjolfsson, 2017).

The three domains are mutually dependent: Data Science provides the data and methods, AI provides learning and inference capability, and automation operationalises AI outputs at scale within business and public processes. This interdependence implies that ethical, data-governance, security and workforce risks are also interconnected, a premise that underpins the integrated framework proposed in Section 7.

4. Responsible and Ethical Artificial Intelligence.

4.1 Concept and Convergence of Principles

Responsible AI refers to the design, development, deployment and governance of AI systems in a manner consistent with ethical principles, legal obligations, human rights and societal values (Floridi et al., 2018). It goes beyond technical accuracy to address how AI affects individuals, organisations and society. A review of 84 AI ethics guidelines identified global convergence around five principles: transparency, justice and fairness, non-maleficence, responsibility and privacy (Jobin et al., 2019). Similar principles appear in the European Commission's High-Level Expert Group guidelines for trustworthy AI (High-Level Expert Group on Artificial Intelligence [HLEG], 2019), the OECD Recommendation on AI (OECD, 2019c), and UNESCO's Recommendation on the Ethics of AI (UNESCO, 2021). Floridi and Cows (2019) consolidate them into five principles (beneficence, non-maleficence, autonomy, justice and explicability), while Fjeld et al. (2020) map a comparable consensus across rights-based documents.

The literature also cautions that principles alone are insufficient. Hagendorff (2020) argues that many guidelines lack enforcement mechanisms, and Morley et al. (2020) document a persistent gap between high-level principles and practical tools. The following subsections therefore discuss each principle together with the mechanisms that operationalise it.

4.2 Fairness and Non-Discrimination

Fairness requires that AI systems do not produce unjustified disparate outcomes for individuals or groups defined by attributes such as gender, ethnicity, age or socio-economic status. Bias may originate in historical data reflecting past discrimination, in unrepresentative sampling, in proxy variables or in feedback loops (Barocas & Selbst, 2016; Friedman & Nissenbaum, 1996; Mehrabi et al., 2022). Empirical audits have shown, for example, that commercial gender-classification systems had error rates of up to 34.7 per cent for darker-skinned women compared with 0.8 per cent for lighter-skinned men (Buolamwini & Gebru, 2018), and that a widely used healthcare algorithm under-estimated the needs of Black patients because it used healthcare cost as a proxy for health need (Obermeyer et al., 2019). Selbst et al. (2019) further warn that fairness cannot be achieved by abstract mathematical definitions alone; it must account for the socio-technical context of deployment. Mitigation therefore combines representative data, bias-aware model design and evaluation, fairness metrics appropriate to the context, and regular independent audits.

4.3 Transparency and Explainability

Transparency refers to the ability of stakeholders to understand how an AI system functions and why it produces

a particular output. Explainable AI (XAI) is particularly important in high-stakes applications where decisions must be justified to users, regulators and affected persons (Doshi-Velez & Kim, 2017; Adadi & Berrada, 2018). Techniques range from inherently interpretable models to post-hoc, model-agnostic explanation methods such as LIME (Ribeiro et al., 2016) and SHAP (Lundberg & Lee, 2017), as well as counterfactual explanations that tell individuals what would have to change to obtain a different outcome (Wachter et al., 2018). Barredo Arrieta et al. (2020) emphasise that explainability must be tailored to the audience, since the explanation needed by a developer differs from that needed by a regulator or a data subject.

4.4 Accountability and Auditability

Accountability requires that identifiable humans and organisations remain answerable for AI-driven decisions and their consequences (HLEG, 2019). In practice, accountability depends on documentation and traceability. Model cards (Mitchell et al., 2019) and datasheets for datasets (Gebru et al., 2021) provide standardised documentation of intended use, performance and limitations, while end-to-end internal audit frameworks embed review gates throughout development (Raji et al., 2020). Organisations should also define roles, escalation procedures and redress mechanisms for AI-related harm.

4.5 Human Oversight and Control

Human-in-the-loop and human-on-the-loop arrangements are intended to prevent over-reliance on automated decisions and to allow humans to intervene, override or audit AI outputs. Shneiderman (2020) argues that elevated levels of automation and elevated levels of human control are compatible when systems are designed for reliability, safety and trustworthiness. Article 14 of the EU AI Act makes human oversight a legal requirement for high-risk systems (Regulation (EU) 2024/1689, 2024). However, oversight must be meaningful: Bainbridge's (1983) "ironies of automation" show that operators who rarely intervene may lose the skills and situational awareness needed when intervention is required, which links human oversight directly to workforce training (Section 6).

4.6 Safety, Robustness and Reliability

AI systems must perform reliably under normal and adversarial conditions. Amodei et al. (2016) identify concrete safety problems, including negative side effects, reward hacking and robustness to distributional shift. International standards now provide risk-management guidance specific to AI, notably ISO/IEC 23894:2023 on AI risk management and ISO/IEC 42001:2023 on AI management systems (ISO/IEC, 2023a, 2023b), complemented by the NIST AI Risk Management Framework (National Institute of Standards and Technology

[NIST], 2023), which organises activities around the functions Govern, Map, Measure and Manage.

4.7 From Principles to Organisational AI Governance

Organisational AI governance comprises the rules, practices, processes and technological tools used to ensure that an organisation's use of AI aligns with its strategies, objectives and values, and with legal requirements and ethical principles (Mäntymäki et al., 2022). A recent review distinguishes structural practices (for example, ethics committees and defined roles), procedural practices (for example, impact assessments, audits and documentation) and relational practices (for example, stakeholder engagement and training) (Papagiannidis et al., 2025). Typical mechanisms include AI ethics or risk committees, pre-deployment impact assessments, documentation and traceability, and continuous post-deployment monitoring. Regulation is increasingly converting these voluntary practices into obligations. The EU Artificial Intelligence Act

(Regulation (EU) 2024/1689, 2024) establishes a risk-based regime that prohibits certain practices, imposes data-governance, documentation, transparency and human-oversight requirements on high-risk systems, and regulates general-purpose AI models (Veale & Zuiderveen Borgesius, 2021). In July 2026, the EU adopted Digital Omnibus on AI, which amended the Act and deferred the application dates of several high-risk obligations (Regulation (EU) 2026/1744, 2026). Public-sector deployments raise additional legitimacy concerns because automated decisions can affect citizens' rights directly (Kuziemski & Misuraca, 2020; Wirtz et al., 2019).

4.8 Evidence from International Case Studies

Table 1 summarises documented international cases that illustrate the ethical risks discussed above. The cases were selected because each is supported by peer-reviewed analysis, judicial or regulatory records, or investigative reporting by established outlets.

Table 1. Selected international case studies on responsible and ethical AI

S/ N	Case / application	Period	Jurisdiction	Key ethical and governance issues	Source
1	AI system for breast-cancer screening (Google Health and partners)	2020	UK / US	External validity across populations, clinical validation, human–AI division of labour, patient safety	McKinney et al. (2020)
2	Royal Free NHS Trust – Google DeepMind (Streams app)	2015–2017	UK	Lawful basis and transparency for sharing identifiable patient records; ICO found a breach of data-protection law	Powles & Hodson (2017)
3	Clearview AI facial-recognition database	2020–2024	France; Netherlands (and others)	Scraping of facial images without consent; biometric data processing; regulatory fines of €20 m (CNIL) and €30.5 m (Dutch AP)	European Data Protection Board (2022); Autoriteit Persoonsgegevens (2024)
4	Wrongful arrest following facial-recognition match (Detroit)	2020	US	Misidentification, over-reliance on automated matches, due process	Hill (2020)
5	Amazon experimental recruitment tool	2014–2017 (reported 2018)	US	Gender bias learned from historical hiring data; project abandoned	Dastin (2018)
6	COMPAS recidivism risk assessment	2016	US	Racial disparities in error rates; opacity of proprietary scoring	Angwin et al. (2016)
7	Predictive policing (PredPol) simulation	2016	US	Feedback loops reinforcing over-policing of minority neighbourhoods	Lum & Isaac (2016)
8	Healthcare risk-prediction algorithm	2019	US	Racial bias arising from cost used as a proxy for health need	Obermeyer et al. (2019)
9	SyRI welfare-fraud risk system	2014–2020	Netherlands	Opaque profiling of low-income neighbourhoods; struck down as violating the right to private life (Art. 8 ECHR)	van Bekkum & Zuiderveen Borgesius (2021); Rechtbank Den Haag (2020)
10	Social Credit System	2014–present	China	State surveillance infrastructure, limited transparency and contestability	Liang et al. (2018); Creemers (2018)
11	Barcelona digital-city and data-sovereignty programme	2016–2019	Spain	Positive case: citizen-centred data governance and data sovereignty for public value	Monge et al. (2022)

4.9 Evidence from Nigeria

Nigeria offers an instructive case of an emerging digital economy in which AI-enabled and data-intensive systems have been deployed rapidly in identity management,

elections, financial services and telecommunications. Table 2 summarises documented cases; all involve large-scale processing of personal or biometric data, and several have resulted in regulatory enforcement.

Table 2. Responsible AI and data-governance case studies in Nigeria

S/ N	Case / application	Period	Key ethical and governance issues	Source
1	Bimodal Voter Accreditation System (BVAS) and INEC Result Viewing portal (IReV), 2023 general elections	2023	Biometric (fingerprint and facial) voter authentication; delays in uploading presidential result forms reduced transparency and public trust	Electoral Act (2022, s. 47(2)); European Union Election Observation Mission (2023)
2	National Identity Number (NIN) ecosystem and third-party identity-verification websites	2024	Alleged sale of NIN-linked personal data via verification sites; NIMC denied any breach of its database; concerns over access controls for KYC services	Macdonald (2024)
3	Digital lending applications (Soko Lending case)	2019–2021	Excessive data harvesting, trackers sharing data with third parties, privacy-invading messages to borrowers' contacts; ₦10 m fine under the NDPR	Nairametrics (2021)
4	Regulation of digital lenders	2025	Registration and conduct rules for digital lenders, including data and debt-recovery practices	Federal Competition and Consumer Protection Commission (2025)
5	Fidelity Bank Plc	2024	Violations of the NDPR 2019 and the NDPA 2023; ₦555.8 m fine by the NDPC	Aro (2024)
6	Meta Platforms / WhatsApp	2024–2025	Privacy-policy and data practices found to contravene Nigerian law; US\$220 m FCCPC penalty upheld by the Competition and Consumer Protection Tribunal	Aro (2025)
7	MultiChoice Nigeria	2025	Processing of subscribers' and non-subscribers' data and unlawful cross-border transfer; ₦766 m fine by the NDPC	Okogba (2025)

4.10 Nigeria-specific insights

Four insights emerge from the Nigerian evidence. First, there is a governance gap: Nigeria had not enacted an AI-specific statute at the time of writing, and AI systems are governed principally through the Nigeria Data Protection Act 2023 (NDPA) and its General Application and Implementation Directive (Nigeria Data Protection Commission [NDPC], 2025), complemented by sectoral regulators and a National Artificial Intelligence Strategy first published in draft in 2024 (Federal Ministry of Communications, Innovation and Digital Economy [FMCIDE] & National Information Technology Development Agency [NITDA], 2024). Second, privacy and consent are the dominant ethical concerns in documented Nigerian cases, ahead of risks associated with highly autonomous systems. Third, public trust is fragile: the BVAS/IReV experience shows that technical deployment does not by itself secure legitimacy without transparency and accountability (European Union Election Observation Mission, 2023). Fourth, enforcement is strengthening: the significant penalties imposed on Fidelity Bank, Meta and

MultiChoice indicate a shift from a predominantly reactive posture towards more assertive regulation (Aro, 2024, 2025; Okogba, 2025). These findings are consistent with broader analyses of AI in Africa that emphasise data-governance capacity, contextual fairness and the risk of importing systems designed for other contexts (Birhane, 2020; Gwagwa et al., 2020; Eke et al., 2023).

5. DATA GOVERNANCE, PRIVACY AND CYBERSECURITY IN AI-DRIVEN SYSTEMS

5.1 Data Governance as the Foundation of Trustworthy AI

Data governance is the framework of decision rights, accountabilities, policies, standards and processes that ensure data are managed as an asset throughout their lifecycle, from collection and storage to processing, sharing and disposal (Khatri & Brown, 2010; Abraham et al., 2019). Because the quality, integrity and representativeness of data directly determines model accuracy, fairness and robustness,

effective data governance is a prerequisite for trustworthy AI (Janssen et al., 2020). Weak data governance results in poor data quality, regulatory non-compliance, biased outcomes and increased exposure to cybersecurity threats.

5.2 Core Components of Data Governance

i. Data ownership and stewardship. Clearly assigned ownership and stewardship roles create accountability for data quality, access control and ethical use (DAMA International, 2017; Khatri & Brown, 2010).

ii. Data Quality Management. Data quality is multidimensional, encompassing intrinsic, contextual, representational and accessibility dimensions such as accuracy, completeness, timeliness and consistency (Wang & Strong, 1996). Poor-quality data propagate errors and bias through AI systems and lead to flawed decisions (Redman, 2008).

iii. Metadata, Provenance and Documentation. Documenting the origin, composition, collection process and intended uses of datasets supports reproducibility and accountability; datasheets for datasets provide a practical template (Gebru et al., 2021).

iv. Data Lifecycle Management. Policies should define how data are collected, stored, processed, archived and securely disposed of, ensuring that personal data are retained only as long as necessary (Khatri & Brown, 2010).

v. Compliance and Regulatory Alignment. Data governance must align with applicable law. The General Data Protection Regulation (GDPR) codifies lawfulness, purpose limitation, data minimisation, accountability and data protection by design and by default (Regulation (EU) 2016/679, 2016; Voigt & von dem Bussche, 2017), and the EU AI Act adds explicit data and data-governance requirements for the training, validation and testing data of high-risk AI systems (Regulation (EU) 2024/1689, 2024). In Nigeria, the NDPA 2023 establishes equivalent principles and created the NDPC as the supervisory authority (Nigeria Data Protection Act, 2023).

5.3 Privacy Challenges in AI and Data Science

Privacy is a central concern because AI systems rely on large volumes of personal, sensitive and, increasingly, biometric data. Solove (2008) conceptualises privacy as a plurality of related problems arising from information collection, processing, dissemination and invasion, while Nissenbaum (2004) frames privacy as contextual integrity: information flows should conform to the norms of the context in which data were shared. Business models built on large-scale behavioural data extraction intensify these concerns (Zuboff, 2019). Key privacy challenges include:

- Excessive collection and secondary use of data beyond the original purpose;

- Lack of meaningful informed consent and transparency;
- Re-identification of individuals from supposedly anonymised datasets; and
- Inference of sensitive attributes from aggregated data drawn from multiple sources.

Re-identification risk is particularly well documented. Narayanan and Shmatikov (2008) de-anonymised subscribers in the Netflix Prize dataset, Ohm (2010) describes the broader failure of anonymisation, and Rocher et al. (2019) estimate that 99.98 per cent of Americans could be correctly re-identified in any dataset using 15 demographic attributes.

5.4 Privacy-Enhancing Techniques

- **Anonymisation and pseudonymisation.** Anonymisation removes identifying attributes, while pseudonymisation replaces identifiers with artificial keys. Formal models such as k -anonymity (Sweeney, 2002) reduce, but do not eliminate, the risk of linkage attacks when datasets are combined (Narayanan & Shmatikov, 2008).
- **Differential Privacy.** Differential privacy provides a mathematical guarantee that the output of an analysis changes only negligibly whether or not any single individual's data are included, typically by adding calibrated noise (Dwork, 2008; Dwork & Roth, 2014). It has been adapted to deep-learning training (Abadi et al., 2016).
- **Federated Learning.** Federated learning trains models across decentralised devices or institutions without transferring raw data to a central server, reducing privacy exposure in sectors such as healthcare and mobile services (McMahan et al., 2017). It does not remove all risk, however, because model updates can still leak information and must be combined with secure aggregation or differential privacy.

5.5 Cybersecurity Risks in AI-driven Environments

The deployment of AI-driven technologies in energy and all its related industries results in risks in cyberattacks and attacks against these industries and others become prevalent and can lead to widespread power outage to physical infrastructural damage (Boye et al, 2024). AI introduces attack surfaces that extend beyond those of conventional information systems because data, models and outputs can each be targeted (Papernot et al., 2018; Biggio & Roli, 2018). Key AI-specific threats include:

- **Data poisoning**, in which adversaries manipulate training data to degrade or bias model behaviour (Biggio & Roli, 2018);
- **Adversarial (evasion) attacks**, in which small, deliberately crafted input perturbations cause incorrect predictions (Goodfellow et al., 2015);

- **Model Extraction**, in which attackers reconstruct proprietary models through prediction interfaces (Tramèr et al., 2016);
- **Model Inversion and Membership inference**, which expose sensitive training data or reveal whether a person's record was used in training (Fredrikson et al., 2015; Shokri et al., 2017); and
- **Automation Abuse**, in which automated processes are exploited at scale.

These threats can compromise system integrity, safety and trust, especially in critical infrastructure and autonomous systems.

5.6 AI for Cybersecurity Enhancement

AI also strengthens cyber defense. Machine-learning and data-mining methods can analyse large volumes of network and host data to detect intrusions and anomalies, classify malware and support automated incident response (Buczak & Guven, 2016; Sarker et al., 2020). Typical applications include intrusion detection and prevention, behavioural malware analysis, automated threat intelligence and continuous risk monitoring. Reliance on AI-based defenses must nevertheless be balanced by human oversight to manage false positives, model drift and adversarial manipulation of the defensive models themselves.

5.7 Privacy and Security by Design

Privacy and security must be embedded throughout the AI lifecycle rather than added after deployment. The privacy-by-design principles articulated by Cavoukian (2011) are

now reflected in the GDPR's requirement for data protection by design and by default (Regulation (EU) 2016/679, 2016). Information-security management systems certified to ISO/IEC 27001:2022 (ISO/IEC, 2022), AI risk management under ISO/IEC 23894 and the NIST AI RMF provide complementary controls (ISO/IEC, 2023a; NIST, 2023). Effective mechanisms include regular security audits and penetration testing, AI-specific threat modelling, data-protection impact assessments, clear incident-response and accountability structures, and close coordination between data-governance, privacy and security functions.

5.8 Interdependence of Data Governance, Privacy and Cybersecurity

Data governance, privacy and cybersecurity are interdependent pillars of trustworthy AI. Strong data governance supports privacy and security by enforcing controlled access, data minimisation and data quality, whereas weak governance amplifies both privacy breaches and cyber risk (Janssen et al., 2020). An integrated approach that aligns governance policies, privacy safeguards and security controls is therefore essential for sustainable and ethical AI deployment.

5.9 Comparative Analysis Across Jurisdictions

Table 3 compares the principal data-protection and AI-governance instruments of the ten jurisdictions studied, and Table 4 presents the authors' qualitative synthesis for the five jurisdictions examined in great depth.

Table 3. Data protection and AI governance instruments in ten jurisdictions

Jurisdiction	Core data-protection law	Supervisory authority	AI-specific instruments or guidance	Illustrative enforcement or evidence
Nigeria	Nigeria Data Protection Act 2023; NDPR 2019; GAID 2025	Nigeria Data Protection Commission (NDPC)	National AI Strategy (draft, 2024); no AI-specific statute	NDPC fines on Fidelity Bank (2024) and MultiChoice (2025); FCCPC penalty on Meta (2024)
Ghana	Data Protection Act 2012 (Act 843)	Data Protection Commission	None identified in this review	—
Kenya	Data Protection Act 2019 (No. 24 of 2019)	Office of the Data Protection Commissioner (ODPC)	None identified in this review	—
Rwanda	Law No. 058/2021 on the protection of personal data and privacy	National Cyber Security Authority (NCSA)	National AI Policy (2023)	—
United States	No comprehensive federal law; sectoral laws and state laws, e.g. CCPA (2018) as amended by CPRA	Sectoral regulators, state attorneys-general and the California Privacy Protection Agency	NIST AI RMF 1.0 (2023, voluntary); Executive Order 14179 (2025)	Equifax breach affecting about 145.5 million people (U.S. Government Accountability Office, 2018)
United Kingdom	UK GDPR; Data Protection Act 2018; Data (Use and Access) Act 2025	Information Commissioner's Office (ICO)	ICO guidance on AI and data protection	ICO finding against Royal Free–DeepMind data sharing (2017)

Jurisdiction	Core data-protection law	Supervisory authority	AI-specific instruments or guidance	Illustrative enforcement or evidence
Spain	GDPR and national implementing law	Spanish Data Protection Agency (AEPD); AI supervision agency AESIA (Statute: Royal Decree 729/2023)	EU AI Act	Barcelona data-sovereignty programme (Monge et al., 2022)
France	GDPR; Loi n° 78-17 (Informatique et Libertés)	CNIL	EU AI Act; CNIL recommendations on AI development (2024–2025)	CNIL €20 m fine on Clearview AI (2022)
Germany	GDPR; Federal Data Protection Act (BDSG) 2017	Federal Commissioner (BfDI) and state authorities	EU AI Act	—
China	Personal Information Protection Law (2021), within a framework including the Cybersecurity Law and Data Security Law	Cyberspace Administration of China (CAC) and other bodies	Interim Measures for the Management of Generative AI Services (2023)	Social Credit System (Liang et al., 2018)

Note. Sources: Nigeria Data Protection Act (2023); NDPC (2025); FMCIDE & NITDA (2024); Data Protection Act, 2012 (Act 843); Data Protection Act No. 24 of 2019 (Kenya); Law No. 058/2021 (2021, Rwanda); Ministry of ICT and Innovation (2023); California Consumer Privacy Act of 2018; NIST (2023); Executive Order 14179 (2025); U.S. Government Accountability Office (2018); Data Protection Act 2018; Data (Use and Access) Act 2025; Information Commissioner's Office (2023); Real Decreto 729/2023 (2023); Loi n° 78-17 (1978); Commission Nationale de l'Informatique et des Libertés (2024); Bundesdatenschutzgesetz (2017); Personal Information Protection Law (2021); Cyberspace Administration of China et al. (2023). A dash indicates that no case was examined in this study, not that none exists.

Table 4. Qualitative comparison of AI-related data governance (authors' synthesis)

Dimension	Nigeria	United States	United Kingdom	Spain (EU)	China
Governance model	Emerging, data-protection-led	Sectoral and market-led	Rights-based (UK GDPR)	Rights-based and risk-based (GDPR + AI Act)	State-centric
Typical AI uses examined	Biometric ID, election technology, digital lending, banking	Credit, recruitment, criminal justice, health	Health, public-sector analytics	Smart city, public services	Social credit, facial recognition
Consent and transparency	Formal requirements; limited transparency in public systems	Varies by state and sector	Explicit legal requirements	Strong legal requirements	Subordinate to state objectives
Enforcement pattern	Increasingly assertive since 2024	Litigation and agency action	Regulator findings and sanctions	Regulatory supervision and audits	Administrative and policy-driven
Principal risks	Consent deficits, data leakage, capacity gaps	Breaches, algorithmic bias, fragmentation	Data-sharing governance	Implementation complexity	Mass surveillance, limited contestability
Overall maturity (authors' assessment)	Low to moderate	Moderate to high	High	High	High state capacity; low individual protection

Note. Assessments are interpretive and derived from the evidence in Tables 1–3; they are intended to support discussion rather than to provide a measured index.

Three comparative insights follow. First, Nigeria is characterised by rapid deployment of data-intensive systems with a governance lag, which makes privacy and cybersecurity the dominant concerns. Second, the United States combines technological leadership with regulatory fragmentation, relying heavily on voluntary frameworks such as the NIST AI RMF (NIST, 2023). Third, the United Kingdom and EU member states such as Spain operate rights-based regimes with independent supervisory authorities, whereas China's model prioritises state security and control over individual privacy (Roberts et al., 2021). Across all jurisdictions, AI tends to intensify existing weaknesses in data governance rather than creating entirely new categories of risk.

6. AUTOMATION, THE FUTURE OF WORK AND WORKPLACE UPSKILLING

6.1 Automation in the Era of Artificial intelligence

With the integration of AI and Data Science, automation has evolved from rule-based systems into intelligent automation capable of learning, adapting and making context-aware decisions, extending automation beyond routine tasks into cognitive and analytical domains (Willcocks et al., 2017; Syed et al., 2020). AI-driven automation includes RPA, intelligent process automation, machine-learning-enabled decision systems and autonomous systems, deployed to optimise workflows, reduce costs, improve accuracy and scale operations in manufacturing, finance, healthcare, energy and public administration (Davenport & Ronanki, 2018). Because automation also brings workforce displacement, skill obsolescence and organisational restructuring, it should be managed as a socio-technical transformation rather than a purely technological initiative.

6.2 Types and Levels of Automation

Drawing on the levels-of-automation perspective (Parasuraman et al., 2000), three broad levels can be distinguished:

Task Automation: automation of repetitive, rules-based activities such as data entry, invoice processing and report generation, commonly using RPA without significant process redesign (van der Aalst et al., 2018).

Process Automation: integration of automated tasks across end-to-end workflows, incorporating natural language processing and predictive analytics to handle semi-structured and unstructured data (Willcocks et al., 2017).

Cognitive and Autonomous Automation: systems that perform complex functions such as decision-making and optimisation with limited human intervention, including predictive maintenance and decision-support platforms, which raise the most significant ethical, governance and accountability questions (Russell & Norvig, 2021).

6.3 Automation and Employment

The relationship between automation and employment has been extensively debated. Frey and Osborne (2017) estimated that about 47 per cent of US employment was at substantial risk of computerisation. Task-based analyses produced substantially lower estimates: Arntz et al. (2016) found that, on average, 9 per cent of jobs across 21 OECD countries were automatable, and Nedelkoska and Quintini (2018) estimated that about 14 per cent of jobs were highly automatable, with a further 32 per cent likely to change significantly. The task-based framework explains these differences: technology substitutes for routine tasks while complementing non-routine analytical and interpersonal tasks (Autor et al., 2003; Autor, 2015). Acemoglu and Restrepo (2019) show that automation displaces labour from some tasks but that the creation of new tasks can reinstate labour demand. Nevertheless, effects can be negative locally: Acemoglu and Restrepo (2020) estimate that each additional robot per thousand workers reduced the US employment-to-population ratio by 0.2 percentage points and wages by 0.42 per cent.

6.4 Generative AI and the changing exposure of work

Generative AI extends automation potential to cognitive, non-routine tasks previously considered relatively protected. Eloundou et al. (2024) finds that large language models could affect a substantial share of tasks across a wide range of occupations, including higher-wage occupations. The International Labour Organization concludes that clerical work is the most exposed occupational group and that augmentation is more likely than full automation for most occupations (Gmyrek et al., 2023). Experimental and field studies report productivity gains: access to a generative AI assistant improved productivity in professional writing tasks (Noy & Zhang, 2023) and in customer support, where the gains were largest for less experienced and less skilled workers (Brynjolfsson et al., 2025). These findings suggest that the distributional effects of AI depend heavily on how it is deployed and on complementary investment in skills.

6.5 The Future of Work in an AI-driven Economy

The future of work is increasingly defined by human–AI collaboration, flexible work arrangements and continuous skill adaptation (Daugherty & Wilson, 2018; OECD, 2019a). Employers surveyed by the World Economic Forum expect AI and information-processing technologies to have the greatest impact of any technology, with 86 per cent of respondents expecting them to transform their business by 2030, and 58 per cent expecting robots and autonomous systems to do so (WEF, 2025). Key characteristics of the emerging workplace include hybrid human–machine work models, digitally enabled collaboration, data-driven decision-making and an emphasis on adaptability and

lifelong learning. Organisations must accordingly redesign job roles, performance metrics and leadership models.

6.6 Organisational Transformation and Workforce Readiness

Automation-driven transformation requires changes in organisational culture, governance and talent management, not only technology adoption. Resistance often stems from fear of job loss, lack of digital skills and inadequate communication, so structured management change is essential (Kotter, 2012). Organisations that navigate automation successfully involve employees in technology deployment, communicate transparently and align automation with broader organisational goals (Morandini et al., 2023).

6.7 Workplace Upskilling and Reskilling

Upskilling enhances employees' existing skills, whereas reskilling prepares them for distinct roles; both are essential for maintaining employability as task content changes (OECD, 2019b; Li, 2024). Morandini et al. (2023) review evidence that AI is reshaping the skills required of workers and argues that organisations must invest systematically in upskilling and reskilling. Future-ready skills include data literacy and analytical reasoning; foundational

understanding of AI and machine-learning concepts, including their limitations; cybersecurity and digital-risk awareness; ethical reasoning and governance literacy; and creativity, adaptability, collaboration and complex problem-solving. Because the pace of change outstrips traditional education pathways, lifelong learning models that combine formal education with micro-credentials, online learning, industry certification and workplace-based training are increasingly important (OECD, 2019b; WEF, 2023). Governments, employers and educational institutions share responsibility for building inclusive learning ecosystems that reduce skill gaps and widen access to digital opportunity.

6.8 The Role of Policy and Institutions

Public policy shapes how automation affects workers. Governments can support transitions through education reform, active labour-market policies, social protection and public–private partnerships, together with investment in digital infrastructure (OECD, 2019a). The IMF recommends that emerging market and developing economies, a group that includes Nigeria, prioritise digital infrastructure and digital skills so that they are not left behind (Cazzaniga et al., 2024). Table 5 compares flagship workforce and upskilling initiatives in the jurisdictions studied.

Table 5: Comparative Overview of Automation, Future-of-Work and Upskilling Initiative

Country	Flagship policy or initiative	Upskilling emphasis	Key gaps and risks (authors' assessment)	Source
Nigeria	National Digital Economy Policy and Strategy 2020–2030; Three Million Technical Talent (3MTT) programme (launched 2023); National AI Strategy (draft, 2024)	Mass digital literacy; software, data and AI foundations	Converting training into jobs; broadband and power infrastructure; SME adoption; training quality assurance	Federal Ministry of Communications and Digital Economy (2019); FMCIDE & NITDA (2024)
United States	Executive Order 14277 on AI education (2025)	AI literacy in education; workforce readiness	Fragmented skills system; unequal access	Executive Order 14277 (2025)
United Kingdom	AI Opportunities Action Plan (2025)	AI skills and talent pipeline	Uneven employer investment in training	Department for Science, Innovation and Technology (2025)
Spain	National Digital Skills Plan (Plan Nacional de Competencias Digitales, 2021)	Basic-to-advanced digital skills; vocational upskilling	ICT-specialist shortage; regional and SME disparities	Gobierno de España (2021)
France	National AI strategy "AI for Humanity" (2018)	AI research talent and training	Scaling training nationally; SME adoption	Villani (2018)
Germany	Industrie 4.0 strategic initiative	Advanced technical, automation and industrial-data skills	Demographic pressure; pace of retraining; SME integration	Kagermann et al. (2013)
Rwanda	National AI Policy (2023), including a 21st-century skills and AI literacy priority	AI literacy; digital-government skills	Small labour market; depth of advanced-skills pipeline	Ministry of ICT and Innovation (2023)
Kenya	Ajira Digital programme (2016)	Online and digital work skills; employability	Earnings volatility and protection in platform work	Ajira Digital (n.d.)

The comparison indicates that European countries generally rely on structured national programmes backed by stronger institutional capacity, whereas African programmes prioritise youth employability, digital jobs and mass digital literacy; the principal challenge in the latter is converting training into stable employment. Globally, employers expect AI and information processing, together with robotics and autonomous systems, to be major drivers of workforce change (WEF, 2025).

7. AN INTEGRATED RESPONSIBLE AUTOMATION FRAMEWORK (IRAF)

7.1 Structure of the Framework

Synthesising Sections 4–6, this paper proposes the Integrated Responsible Automation Framework (IRAF), illustrated in Figure 1. The framework rests on two premises established in the review: that data governance is the foundation on which ethical, secure and effective AI depends (Janssen et al., 2020; Abraham et al., 2019), and that ethical, security and workforce risks are interdependent and therefore require coordinated rather than siloed responses (Papagiannidis et al., 2025).

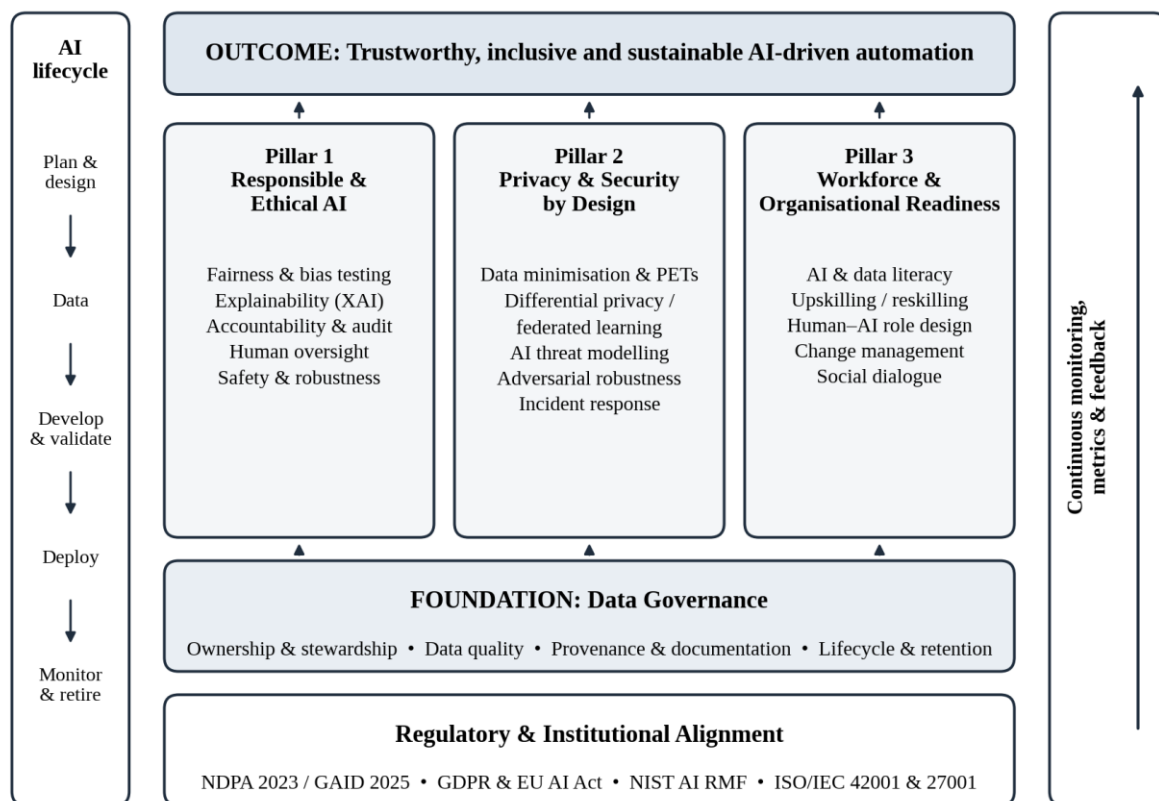


Figure 1. The Integrated Responsible Automation Framework (IRAF). Source: Authors.

The IRAF comprises five layers:

1. **Regulatory and Institutional Alignment (base).** Organisations map their obligations under applicable law (for example, the NDPA 2023 and GAID 2025 in Nigeria, or the GDPR and AI Act in the EU) and adopt recognised management standards such as ISO/IEC 42001 and ISO/IEC 27001 and the NIST AI RMF.
2. **Data Governance (Foundation).** Ownership and stewardship, data quality, provenance and documentation, and lifecycle and retention controls ensure that data used by AI systems are lawful, accurate, representative and secure.
3. **Pillar 1: Responsible and Ethical AI.** Fairness testing, explainability, accountability and audit, human oversight and robustness testing operationalise the principles discussed in Section 4.
4. **Pillar 2: Privacy and Security by design.** Data minimisation, privacy-enhancing technologies, AI-specific threat modelling, adversarial-robustness testing and incident response protect individuals and systems (Section 5).
5. **Pillar 3: Workforce and Organisational Readiness.** AI and data literacy, upskilling and reskilling, human-AI role design, change management and social

dialogue ensure that people can use, oversee and benefit from automation (Section 6).

Two cross-cutting elements connect the layers. The AI lifecycle (plan and design, data, develop and validate, deploy, monitor and retire) determines when each control is

applied, and continuous monitoring and feedback ensure that performance, fairness, security and workforce indicators inform iterative improvement. Table 6 maps the controls to lifecycle stages.

Table 6. Operationalising the IRAF across the AI lifecycle

Lifecycle stage	Data governance	Responsible AI	Privacy and security	Workforce readiness	Supporting references
Plan and design	Define data owners and stewards; assess data availability and lawful basis	Impact assessment; define fairness objectives and accountability	Privacy-by-design requirements; threat model	Engage affected workers; identify role and skill changes	HLEG (2019); Cavoukian (2011); Kotter (2012)
Data	Quality profiling; provenance documentation; retention rules	Representativeness and bias checks	Minimisation; pseudonymisation; access control	Train staff in data handling and literacy	Wang & Strong (1996); Gebru et al. (2021); Sweeney (2002)
Develop and validate	Version control of datasets and models	Fairness metrics; explainability; model cards	Differential privacy or federated learning where appropriate; adversarial testing	Build internal AI and assurance capability	Mitchell et al. (2019); Abadi et al. (2016); Goodfellow et al. (2015)
Deploy	Access governance; lineage tracking	Human-oversight procedures; user information	Security hardening; incident-response plan	Redesign roles; train operators for oversight	Shneiderman (2020); ISO/IEC (2022); Bainbridge (1983)
Monitor and retire	Data-drift monitoring; secure disposal	Periodic audits; complaints and redress	Continuous threat monitoring; breach notification	Reskilling; evaluate workforce outcomes	Raji et al. (2020); NIST (2023); Li (2024)

7.2 Research Propositions

In order to support empirical testing of the framework we presented the following propositions:

P1. The organisations with more mature data governance will report fewer fairness, privacy and security incidents in their AI systems than organisations with less mature data governance.

P2. The positive effect of AI adoption on organisational performance will be stronger where investment in workforce upskilling is higher.

P3. Human oversight will be more effective in preventing harm where operators have received AI-specific training, because training mitigates the “ironies of automation”.

P4. In emerging economies, regulatory enforcement capacity will moderate the relationship between AI adoption and public trust in AI-enabled public services.

7.3 Application to the Nigerian Context

For Nigeria, the framework suggests four key objectives: (i) translating the NDPA 2023 and GAID 2025 to the sector-specific guidance on automated decision-making and AI-

specific data protection impact assessment; (ii) implementing the National AI Strategy with institutional responsibilities, risk classification and audit requirements to be transparent; (iii) strengthening security and access controls at national identity and verification ecosystems in particular (the 2024 allegations show how third-party access points can undermine trust); (iv) linking mass digital-skills programmes such as 3MTT to industry demand, AI literacy and governance skills for employment in the job market. Regional instruments such as the African Union Continental Artificial Intelligence Strategy (African Union, 2024) and the African Union Convention on Cyber Security and Personal Data Protection (African Union, 2014) serve as a basis for harmonised approaches.

8. RESULTS AND DISCUSSIONS

8.1 Theoretical Implications

The review shows that ethical, data-governance, security, and workforce dimensions of AI are interdependent instead of separate from each other. Fairness depends on data quality and representativeness; privacy depends on data governance and security; and meaningful human oversight depends on workforce skills. By positioning data

governance as the basis and developing a set of ideas that link governance maturity and skills investment and regulatory capacity to outcomes, the IRAF extends principle-based AI ethics frameworks (Floridi et al., 2018; Jobin et al., 2019) to an operational, socio-technical setting. It also responds to calls for policy research on AI ethics to move from “what” to “how” (Morley et al., 2020) and governance research in Africa (Eke et al., 2023; Gwagwa et al., 2020).

8.2 Practical Implications.

For policymakers, particularly in Nigeria, the findings point to a need to supplement data-protection law with AI-specific guidance, to provide adequate support to the resource’s supervisory bodies and for digital-skills programs to be aligned with labour market demand. For organisations, the IRAF provides a checklist for embedding controls right through the AI lifecycle and coordination of the data, risk, security, legal and human-resources functions. For educators and training providers, the results show the need for technical AI and data skills combined with ethics and governance and cybersecurity literacy in a professional context.

8.3 Limitations and Future Work.

First, it is not a systematic review but an integrative and not a systematic approach. We have selected the sources purposively and have verified the sources independently, but the search is not complete and selection is not complete. Second, the comparison in Tables 4 and 5 is qualitative and interpretive. Third, the AI governance landscape is changing rapidly, as illustrated by the 2026 amendments to the EU AI Act and the National AI Strategy of Nigeria, and some of the information may become outdated. Future work should test propositions P1-P4 empirically, for instance from Nigerian organisations in banking, telecommunications and energy, produce a measure of maturity of AI governance in African countries and the impact on job opportunities for the work done by upskilling in the country (such as 3MTT). AI, Data Science and Automation are all wonderful opportunities for productivity, innovation and public value for all to gain from, but their benefits are not automatic and are not equally distributed. In this paper we have shown that responsible AI adoption requires four interdependent conditions: ethical AI practice that is operationalised and not taken for granted, data governance and privacy and cybersecurity that are built into the design system; and ongoing investment in upskilling and organisational change in workforce training and training. Nigeria is evidence that data-intensive and data-driven deployment is fast and that there are governance and trust gaps in the process and there is no more data-intensive deployment and there is more regulatory enforcement and enforcement in place. The proposed Integrated Responsible Automation Framework

provides policymakers, organisations and researchers with a structured way to align these conditions across the AI lifecycle. For AI-driven automation to deliver meaningful and long-term socio-economic impact we need to balance innovation with inclusion, accountability and human development.

8.4 Research Propositions.

To support empirical testing of the framework, we advance the following propositions:

- P1. More mature data governance will result in fewer fairness, privacy and security incidents in AI systems than organisations with less mature data governance.
- P2. The positive impact of AI adoption on organisational performance will be greater at organisations where there is more investment in workforce upskilling.
- P3. Good human oversight will work better to prevent harm in the cases where operators have received training in AI-specific because training will eliminate the “ironies of automation.”
- P4. In emerging economies, regulatory enforcement capacity will moderate the relationship between AI adoption and public trust in AI-enabled public services. 7.3 for Nigeria. The framework is based on the following: (i) to translate the NDPA 2023 and GAID 2025 to national recommendations on automated decision-making and AI-specific data protection impact assessment; (ii) to complete and implement the National AI Strategy in terms of institutional oversight, risk classification and audit; (iii) strengthen security and access controls across national identity and verification ecosystems, as the 2024 allegations demonstrate that third-party access points can erode trust (Macdonald, 2024); and (iv) link mass digital-skills programmes such as 3MTT to industry demand, AI literacy and governance skills in order to ensure that training will be utilised and be employable. In addition, regional instruments such as the African Union Continental Artificial Intelligence Strategy (African Union, 2024) and the African Union Convention on Cyber Security and Personal Data Protection (African Union, 2014) drive these discussions. 8.1 Theoretical implications. The review shows that the ethical, data-governance, security and workforce aspects of AI are interdependent rather than separable. Fairness is dependent on data quality and representativeness; privacy is dependent on data governance and security; and human oversight requires staff skills. By taking data governance on board and developing propositions that relate governance maturity, skills investment and regulatory capacity to outcomes, IRAF takes a principle-based AI ethics framework (Floridi et al., 2018; Jobin et al., 2019) in an operational, socio-technical context. It also responds to the call for AI ethics research based on Africa (Morley et al., 2020), and those that are

based on governance in Africa (Eke et al., 2023). 8.2 Practical implications. For policymakers, particularly in Nigeria, the results point to the need for a better understanding of data protection law and AI-specific guidance, to resource supervisory bodies and to align digital-skills programs with labour market requirements in the country. For organisations, the IRAF provides a list of controls to be integrated across the AI lifecycle and to work together on data, risk, security, legal and human-resources functions. For educators and training providers, the findings highlight the relevance of integrating technical AI with data skills and ethics, governance and cybersecurity literacy. 8.3 Limitations and future research. This study has limitations as it is an integrative rather than a systematic review. Although sources were chosen carefully and verified independently, the search was not comprehensive and could be biased and some may have been chosen to get what is available in the data. The comparative findings of Tables 4 and 5 are qualitative and interpretive. The AI governance landscape is changing rapidly, with the changes to the EU AI Act in 2026 and the development of Nigeria's AI Strategy ongoing, and this will make some details of this study outdated in the future. Future work should test propositions P1–P4 empirically -for example through surveys of Nigerian businesses in banking, telecommunications and energy and also the employment outcomes of national upskilling programmes like 3MTT.

9. CONCLUSION

AI, Data Science and Automation are all great opportunities for productivity and innovation and for the public by contrast. But they are not something that is automatically happening or distributed. This paper has shown that responsible AI adoption is achieved through four interdependent conditions: ethical AI practices not just announced but implemented; good data governance; privacy and cybersecurity by design; and ongoing investment in workforce upskilling and organisational change. The data-intensive deployment in Nigeria is fast and the governance and trust gaps present in its governance and trust are still present, but regulatory enforcement is increasing. The proposed Integrated Responsible Automation Framework provides policymakers, organisations and researchers with a framework for linking these conditions to the AI lifecycle. If AI-driven automation is to be successful in achieving broad, long-term socio-economic benefit, it must strike a balance between innovation and inclusion, accountability and human development.

References

1. Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 308–318). ACM. <https://doi.org/10.1145/2976749.2978318>
2. Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49, 424–438. <https://doi.org/10.1016/j.ijinfomgt.2019.07.008>
3. Acemoglu, D., & Restrepo, P. (2019). Automation and new tasks: How technology displaces and reinstates labor. *Journal of Economic Perspectives*, 33(2), 3–30. <https://doi.org/10.1257/jep.33.2.3>
4. Acemoglu, D., & Restrepo, P. (2020). Robots and jobs: Evidence from US labor markets. *Journal of Political Economy*, 128(6), 2188–2244. <https://doi.org/10.1086/705716>
5. Adadi, A., & Berrada, M. (2018). Peeking inside the black box: A survey on explainable artificial intelligence (XAI). *IEEE Access*, 6, 52138–52160. <https://doi.org/10.1109/ACCESS.2018.2870052>
6. African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention; entered into force 8 June 2023). <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>
7. African Union. (2024). *Continental artificial intelligence strategy*. <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>
8. Ajira Digital. (n.d.). *Ajira Digital programme*. Government of Kenya. Retrieved October 1, 2026, from <https://ajiradigital.go.ke>
9. Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). *Concrete problems in AI safety* (arXiv:1606.06565). arXiv. <https://doi.org/10.48550/arXiv.1606.06565>
10. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine bias. *ProPublica*. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
11. Arntz, M., Gregory, T., & Zierahn, U. (2016). *The risk of automation for jobs in OECD countries: A comparative analysis* (OECD Social, Employment and Migration Working Papers No. 189). OECD Publishing. <https://doi.org/10.1787/5jlz9h56dvq7-en>
12. Aro, B. (2024, August 21). NDPC fines Fidelity Bank N555m for 'violating' data privacy laws. *TheCable*. <https://www.thecable.ng/ndpc-fines-fidelity-bank-n555m-for-violating-data-privacy-laws/>

13. Aro, B. (2025, April 25). Nigerian tribunal upholds FCCPC's \$220m fine against Meta. *TheCable*. <https://www.thecable.ng/breaking-tribunal-upholds-fccpcs-220m-fine-against-meta/>
14. Autoriteit Persoonsgegevens. (2024, September 3). *Dutch DPA imposes a fine on Clearview because of illegal data collection for facial recognition*. <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-imposes-a-fine-on-clearview-because-of-illegal-data-collection-for-facial-recognition>
15. Autor, D. H. (2015). Why are there still so many jobs? The history and future of workplace automation. *Journal of Economic Perspectives*, 29(3), 3–30. <https://doi.org/10.1257/jep.29.3.3>
16. Autor, D. H., Levy, F., & Murnane, R. J. (2003). The skill content of recent technological change: An empirical exploration. *The Quarterly Journal of Economics*, 118(4), 1279–1333. <https://doi.org/10.1162/003355303322552801>
17. Bainbridge, L. (1983). Ironies of automation. *Automatica*, 19(6), 775–779. [https://doi.org/10.1016/0005-1098\(83\)90046-8](https://doi.org/10.1016/0005-1098(83)90046-8)
18. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732. <https://doi.org/10.15779/Z38BG31>
19. Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bannetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115. <https://doi.org/10.1016/j.inffus.2019.12.012>
20. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317–331. <https://doi.org/10.1016/j.patcog.2018.07.023>
21. Birhane, A. (2020). Algorithmic colonization of Africa. *SCRIPTed: A Journal of Law, Technology & Society*, 17(2), 389–409. <https://doi.org/10.2966/scrip.170220.389>
22. Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
23. Brynjolfsson, E., Li, D., & Raymond, L. (2025). Generative AI at work. *The Quarterly Journal of Economics*, 140(2), 889–942. <https://doi.org/10.1093/qje/qjae044>
24. Brynjolfsson, E., & McAfee, A. (2014). *The second machine age: Work, progress, and prosperity in a time of brilliant technologies*. W. W. Norton & Company.
25. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. <https://doi.org/10.1109/COMST.2015.2494502>
26. Bundesdatenschutzgesetz [Federal Data Protection Act] (BDSG). (2017). Federal Republic of Germany. https://www.gesetze-im-internet.de/bdsg_2018/
27. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 77–91. <https://proceedings.mlr.press/v81/buolamwini18a.html>
28. Boye, A.F., Taylor, E.O. and Bhagat, D., (2024). AI AND PERFORMANCE CAPABILITIES OF CYBERSECURITY IN THE ENERGY INDUSTRY. *ISAR Journal of Science and Technology*, 2(12), 29–36.
29. California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq. (2018). <https://oag.ca.gov/privacy/ccpa>
30. Cao, L. (2017). Data science: A comprehensive overview. *ACM Computing Surveys*, 50(3), Article 43. <https://doi.org/10.1145/3076253>
31. Cavoukian, A. (2011). *Privacy by design: The 7 foundational principles* (Rev. ed.; original work published 2009). Information and Privacy Commissioner of Ontario. <https://www.sfu.ca/~palys/Cavoukian-2011-PrivacyByDesign-7FoundationalPrinciples.pdf>
32. Cazzaniga, M., Jaumotte, F., Li, L., Melina, G., Panton, A. J., Pizzinelli, C., Rockall, E. J., & Mendes Tavares, M. (2024). *Gen-AI: Artificial intelligence and the future of work* (IMF Staff Discussion Note SDN/2024/001). International Monetary Fund. <https://doi.org/10.5089/9798400262548.006>
33. Chui, M., Hall, B., Mayhew, H., Singla, A., & Sukharevsky, A. (2022, December 6). *The state of AI in 2022—and a half decade in review*. McKinsey & Company. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review>
34. Commission Nationale de l'Informatique et des Libertés. (2024). *Les fiches pratiques IA* [AI how-to sheets]. <https://www.cnil.fr/fr/les-fiches-pratiques-ia>

35. Creemers, R. (2018). *China's Social Credit System: An evolving practice of control* [Preprint]. SSRN. <https://doi.org/10.2139/ssrn.3175792>
36. Cyberspace Administration of China, National Development and Reform Commission, Ministry of Education, Ministry of Science and Technology, Ministry of Industry and Information Technology, Ministry of Public Security, & National Radio and Television Administration. (2023). *Interim measures for the management of generative artificial intelligence services* (China Law Translate, Trans.). <https://www.chinalawtranslate.com/en/generative-ai-interim/>
37. DAMA International. (2017). *DAMA-DMBOK: Data management body of knowledge* (2nd ed.). Technics Publications.
38. Dastin, J. (2018, October 10). Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*. <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>
39. Data (Use and Access) Act 2025, c. 18 (UK). <https://www.legislation.gov.uk/ukpga/2025/18>
40. Data Protection Act 2018, c. 12 (UK). <https://www.legislation.gov.uk/ukpga/2018/12>
41. Data Protection Act, 2012 (Act 843) (Ghana). <https://www.dataprotection.org.gh>
42. Data Protection Act No. 24 of 2019 (Kenya). <https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2022-12-31>
43. Daugherty, P. R., & Wilson, H. J. (2018). *Human + machine: Reimagining work in the age of AI*. Harvard Business Review Press.
44. Davenport, T. H., & Ronanki, R. (2018). Artificial intelligence for the real world. *Harvard Business Review*, 96(1), 108–116. <https://hbr.org/2018/01/artificial-intelligence-for-the-real-world>
45. Department for Science, Innovation and Technology. (2025). *AI opportunities action plan*. UK Government. <https://www.gov.uk/government/publications/ai-opportunities-action-plan>
46. Dhar, V. (2013). Data science and prediction. *Communications of the ACM*, 56(12), 64–73. <https://doi.org/10.1145/2500499>
47. Donoho, D. (2017). 50 years of data science. *Journal of Computational and Graphical Statistics*, 26(4), 745–766. <https://doi.org/10.1080/10618600.2017.1384734>
48. Doshi-Velez, F., & Kim, B. (2017). *Towards a rigorous science of interpretable machine learning* (arXiv:1702.08608). arXiv. <https://doi.org/10.48550/arXiv.1702.08608>
49. Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., . . . Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 57, Article 101994. <https://doi.org/10.1016/j.ijinfomgt.2019.08.002>
50. Dwork, C. (2008). Differential privacy: A survey of results. In *Theory and applications of models of computation (TAMC 2008)* (Lecture Notes in Computer Science, Vol. 4978, pp. 1–19). Springer. https://doi.org/10.1007/978-3-540-79228-4_1
51. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3–4), 211–407. <https://doi.org/10.1561/04000000042>
52. Eke, D. O., Wakunuma, K., & Akintoye, S. (Eds.). (2023). *Responsible AI in Africa: Challenges and opportunities*. Palgrave Macmillan. <https://doi.org/10.1007/978-3-031-08215-3>
53. Electoral Act, 2022 (Nigeria). Federal Republic of Nigeria.
54. Eloundou, T., Manning, S., Mishkin, P., & Rock, D. (2024). GPTs are GPTs: Labor market impact potential of LLMs. *Science*, 384(6702), 1306–1308. <https://doi.org/10.1126/science.adj0998>
55. European Data Protection Board. (2022, October 20). *The French SA fines Clearview AI EUR 20 million*. https://edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en
56. European Union Election Observation Mission. (2023). *Nigeria 2023 general elections: Final report*. European External Action Service. <https://www.eeas.europa.eu/sites/default/files/documents/2023/EU%20EOM%20NGA%202023%20FR.pdf>
57. Executive Order 14179 of January 23, 2025: Removing barriers to American leadership in artificial intelligence. (2025). *Federal Register*, 90, 8741. <https://www.federalregister.gov/documents/2025/01/31/2025-02172/>

58. Executive Order 14277 of April 23, 2025: Advancing artificial intelligence education for American youth. (2025). *Federal Register*, 90, 17519. <https://www.govinfo.gov/content/pkg/FR-2025-04-28/pdf/2025-07368.pdf>
59. Federal Competition and Consumer Protection Commission. (2025). *Digital, Electronic, Online, or Non-Traditional Consumer Lending Regulations*, 2025. <https://fccpc.gov.ng/wp-content/uploads/2025/11/Digital-Electronic-Online-or-Non-Traditional-Consumer-Lending-Regulations-2025.pdf>
60. Federal Ministry of Communications and Digital Economy. (2019). *National digital economy policy and strategy (2020–2030)*. Federal Republic of Nigeria. <https://nitda.gov.ng/wp-content/uploads/2020/11/National-Digital-Economy-Policy-and-Strategy2.pdf>
61. Federal Ministry of Communications, Innovation and Digital Economy & National Information Technology Development Agency. (2024). *National artificial intelligence strategy* [Draft]. https://ncair.nitda.gov.ng/wp-content/uploads/2024/08/National-AI-Strategy_01082024-copy.pdf
62. Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Sriksumar, M. (2020). *Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI* (Berkman Klein Center Research Publication No. 2020-1). Berkman Klein Center for Internet & Society, Harvard University. <https://doi.org/10.2139/ssrn.3518482>
63. Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review*, 1(1). <https://doi.org/10.1162/99608f92.8cd550d1>
64. 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>
65. Fredrikson, M., Jha, S., & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1322–1333). ACM. <https://doi.org/10.1145/2810103.2813677>
66. Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, 114, 254–280. <https://doi.org/10.1016/j.techfore.2016.08.019>
67. Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems*, 14(3), 330–347. <https://doi.org/10.1145/230538.230561>
68. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, 64(12), 86–92. <https://doi.org/10.1145/3458723>
69. Gmyrek, P., Berg, J., & Bescond, D. (2023). *Generative AI and jobs: A global analysis of potential effects on job quantity and quality* (ILO Working Paper No. 96). International Labour Organization. <https://doi.org/10.54394/FHEM8239>
70. Gobierno de España. (2021). *Plan Nacional de Competencias Digitales* [National Digital Skills Plan]. Ministerio de Asuntos Económicos y Transformación Digital. https://portal.mineco.gob.es/recursosarticulo/mineco/ministerio/ficheros/210127_plan_nacional_de_competencias_digitales.pdf
71. Goodfellow, I. J., Shlens, J., & Szegedy, C. (2015). *Explaining and harnessing adversarial examples* [Conference paper]. 3rd International Conference on Learning Representations (ICLR 2015), San Diego, CA, United States. <https://doi.org/10.48550/arXiv.1412.6572>
72. Gwagwa, A., Kraemer-Mbula, E., Rizk, N., Rutenberg, I., & de Beer, J. (2020). Artificial intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions. *The African Journal of Information and Communication*, 26, 1–28. <https://doi.org/10.23962/10539/30361>
73. Hagendorff, T. (2020). The ethics of AI ethics: An evaluation of guidelines. *Minds and Machines*, 30(1), 99–120. <https://doi.org/10.1007/s11023-020-09517-8>
74. High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*. European Commission. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>
75. Hill, K. (2020, June 24). Wrongfully accused by an algorithm. *The New York Times*. <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

76. 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/>
77. ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization. <https://www.iso.org/standard/27001>
78. ISO/IEC. (2023a). *ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management*. International Organization for Standardization. <https://www.iso.org/standard/77304.html>
79. ISO/IEC. (2023b). *ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system*. International Organization for Standardization. <https://www.iso.org/standard/42001>
80. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly*, 37(3), Article 101493. <https://doi.org/10.1016/j.giq.2020.101493>
81. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399. <https://doi.org/10.1038/s42256-019-0088-2>
82. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, 349(6245), 255–260. <https://doi.org/10.1126/science.aaa8415>
83. Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Securing the future of German manufacturing industry: Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0 Working Group*. acatech – National Academy of Science and Engineering. <https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/>
84. Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, 62(1), 15–25. <https://doi.org/10.1016/j.bushor.2018.08.004>
85. Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, 53(1), 148–152. <https://doi.org/10.1145/1629175.1629210>
86. Kotter, J. P. (2012). *Leading change* (with a new preface by the author). Harvard Business Review Press.
87. Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, 44(6), Article 101976. <https://doi.org/10.1016/j.telpol.2020.101976>
88. Law No. 058/2021 of 13/10/2021 relating to the protection of personal data and privacy. (2021). *Official Gazette of the Republic of Rwanda*. <https://dpo.gov.rw>
89. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. <https://doi.org/10.1038/nature14539>
90. Li, L. (2024). Reskilling and upskilling the future-ready workforce for Industry 4.0 and beyond. *Information Systems Frontiers*, 26(5), 1697–1712. <https://doi.org/10.1007/s10796-022-10308-y>
91. Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4), 415–453. <https://doi.org/10.1002/poi3.183>
92. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law No. 78-17 on Information Technology, Data Files and Civil Liberties]. (1978). Légifrance. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460>
93. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance*, 13(5), 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>
94. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems* (Vol. 30). https://papers.nips.cc/paper_files/paper/2017/hash/8a20a8621978632d76c43dfd28b67767-Abstract.html
95. Macdonald, A. (2024, July 15). Digital rights advocates say Nigeria's NIMC has work to do on data mishandling. *Biometric Update*. <https://www.biometricupdate.com/202407/digital-rights-advocates-say-nigerias-nimc-has-work-to-do-on-data-mishandling>
96. Mäntymäki, M., Minkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, 2(4), 603–609. <https://doi.org/10.1007/s43681-022-00143-x>

97. McAfee, A., & Brynjolfsson, E. (2017). *Machine, platform, crowd: Harnessing our digital future*. W. W. Norton & Company.
98. McKinney, S. M., Sieniek, M., Godbole, V., Godwin, J., Antropova, N., Ashrafian, H., Back, T., Chesus, M., Corrado, G. S., Darzi, A., Etemadi, M., Garcia-Vicente, F., Gilbert, F. J., Halling-Brown, M., Hassabis, D., Jansen, S., Karthikesalingam, A., Kelly, C. J., King, D., . . . Shetty, S. (2020). International evaluation of an AI system for breast cancer screening. *Nature*, 577(7788), 89–94. <https://doi.org/10.1038/s41586-019-1799-6>
99. McMahan, B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. In A. Singh & J. Zhu (Eds.), *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics* (Proceedings of Machine Learning Research, Vol. 54, pp. 1273–1282). PMLR. <https://proceedings.mlr.press/v54/mcmahan17a.html>
100. Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2022). A survey on bias and fairness in machine learning. *ACM Computing Surveys*, 54(6), 1–35. <https://doi.org/10.1145/3457607>
101. Ministry of ICT and Innovation. (2023). *The national AI policy*. Republic of Rwanda. <https://oecd.ai/en/dashboards/policy-initiatives/the-national-ai-policy>
102. Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In *Proceedings of the Conference on Fairness, Accountability, and Transparency* (pp. 220–229). ACM. <https://doi.org/10.1145/3287560.3287596>
103. Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2). <https://doi.org/10.1177/2053951716679679>
104. Monge, F., Barns, S., Kattel, R., & Bria, F. (2022). *A new data deal: The case of Barcelona* (IIPP Working Paper WP 2022/02). UCL Institute for Innovation and Public Purpose. <https://www.ucl.ac.uk/bartlett/public-purpose/publications/2022/feb/new-data-deal-case-barcelona>
105. Morandini, S., Fraboni, F., De Angelis, M., Puzzo, G., Giusino, D., & Pietrantoni, L. (2023). The impact of artificial intelligence on workers' skills: Upskilling and reskilling in organisations. *Informing Science: The International Journal of an Emerging Transdiscipline*, 26, 39–68. <https://doi.org/10.28945/5078>
106. Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and Engineering Ethics*, 26(4), 2141–2168. <https://doi.org/10.1007/s11948-019-00165-5>
107. Nairametrics. (2021, August 19). *NITDA fines online lending platform Sokoloan N10 million for privacy invasion*. <https://nairametrics.com/2021/08/19/nitda-fines-online-lending-platform-sokoloan-n10-million-for-privacy-invasion/>
108. Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy* (pp. 111–125). IEEE. <https://doi.org/10.1109/SP.2008.33>
109. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.AI.100-1>
110. Nedelkoska, L., & Quintini, G. (2018). *Automation, skills use and training* (OECD Social, Employment and Migration Working Papers No. 202). OECD Publishing. <https://doi.org/10.1787/2e2f4ee4-en>
111. Nigeria Data Protection Act, 2023. (2023). Federal Republic of Nigeria. <https://ndpc.gov.ng>
112. Nigeria Data Protection Commission. (2025). *Nigeria Data Protection Act General Application and Implementation Directive (GAID) 2025*. <https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf>
113. Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119–157. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>
114. Noy, S., & Zhang, W. (2023). Experimental evidence on the productivity effects of generative artificial intelligence. *Science*, 381(6654), 187–192. <https://doi.org/10.1126/science.adh2586>
115. Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464), 447–453. <https://doi.org/10.1126/science.aax2342>
116. OECD. (2019a). *OECD employment outlook 2019: The future of work*. OECD Publishing. <https://doi.org/10.1787/9ee00155-en>
117. OECD. (2019b). *OECD skills outlook 2019: Thriving in a digital world*. OECD Publishing. <https://doi.org/10.1787/df80bc12-en>

118. OECD. (2019c). *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449; amended 2024). <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
119. Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57, 1701–1777. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006
120. Okogba, E. (2025, July 7). NDPC fines Multichoice N766m for data breach. *Vanguard*. <https://www.vanguardngr.com/2025/07/ndpc-fines-multichoice-n766m-for-data-breach/>
121. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems*, 34(2), Article 101885. <https://doi.org/10.1016/j.jsis.2024.101885>
122. Papernot, N., McDaniel, P., Sinha, A., & Wellman, M. P. (2018). SoK: Security and privacy in machine learning. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 399–414). IEEE. <https://doi.org/10.1109/EuroSP.2018.00035>
123. Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, 30(3), 286–297. <https://doi.org/10.1109/3468.844354>
124. Personal Information Protection Law of the People's Republic of China. (2021). (DigiChina, Trans.). Stanford University. <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>
125. Powles, J., & Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. *Health and Technology*, 7(4), 351–367. <https://doi.org/10.1007/s12553-017-0179-1>
126. Provost, F., & Fawcett, T. (2013). *Data science for business: What you need to know about data mining and data-analytic thinking*. O'Reilly Media.
127. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33–44). ACM. <https://doi.org/10.1145/3351095.3372873>
128. Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial. (2023). *Boletín Oficial del Estado*, BOE-A-2023-18911. <https://www.boe.es/buscar/doc.php?id=BOE-A-2023-18911>
129. Rechtbank Den Haag [District Court of The Hague]. (2020, February 5). *NJCM et al. v. The State of the Netherlands (SyRI)*, ECLI:NL:RBDHA:2020:1878 [English translation of ECLI:NL:RBDHA:2020:865]. <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878>
130. Redman, T. C. (2008). *Data driven: Profiting from your most important business asset*. Harvard Business Press.
131. 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 and on the free movement of such data (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
132. 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*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
133. Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). (2026). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>
134. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144). ACM. <https://doi.org/10.1145/2939672.2939778>
135. Roberts, H., Cows, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. *AI & Society*, 36(1), 59–77. <https://doi.org/10.1007/s00146-020-00992-2>

136. Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10(1), Article 3069. <https://doi.org/10.1038/s41467-019-10933-3>
137. Russell, S. J., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
138. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 7(1), Article 41. <https://doi.org/10.1186/s40537-020-00318-5>
139. Selbst, A. D., boyd, d., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. In *Proceedings of the Conference on Fairness, Accountability, and Transparency* (pp. 59–68). ACM. <https://doi.org/10.1145/3287560.3287598>
140. Shneiderman, B. (2020). Human-centered artificial intelligence: Reliable, safe & trustworthy. *International Journal of Human-Computer Interaction*, 36(6), 495–504. <https://doi.org/10.1080/10447318.2020.1741118>
141. Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership inference attacks against machine learning models. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 3–18). IEEE. <https://doi.org/10.1109/SP.2017.41>
142. Singla, A., Sukharevsky, A., Yee, L., Chui, M., & Hall, B. (2025, March 12). *The state of AI: How organizations are rewiring to capture value*. McKinsey & Company. <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-how-organizations-are-rewiring-to-capture-value>
143. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
144. Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
145. Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 557–570. <https://doi.org/10.1142/S0218488502001648>
146. Syed, R., Suriadi, S., Adams, M., Bandara, W., Leemans, S. J. J., Ouyang, C., ter Hofstede, A. H. M., van de Weerd, I., Wynn, M. T., & Reijers, H. A. (2020). Robotic process automation: Contemporary themes and challenges. *Computers in Industry*, 115, Article 103162. <https://doi.org/10.1016/j.compind.2019.103162>
147. Torraco, R. J. (2005). Writing integrative literature reviews: Guidelines and examples. *Human Resource Development Review*, 4(3), 356–367. <https://doi.org/10.1177/1534484305278283>
148. Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., & Ristenpart, T. (2016). Stealing machine learning models via prediction APIs. In *25th USENIX Security Symposium (USENIX Security 16)* (pp. 601–618). USENIX Association. <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer>
149. UNESCO. (2021). *Recommendation on the ethics of artificial intelligence* (SHS/BIO/PI/2021/1). <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
150. U.S. Government Accountability Office. (2018). *Data protection: Actions taken by Equifax and federal agencies in response to the 2017 breach* (GAO-18-559). <https://www.gao.gov/products/gao-18-559>
151. van Bekkum, M., & Zuiderveen Borgesius, F. (2021). Digital welfare fraud detection and the Dutch SyRI judgment. *European Journal of Social Security*, 23(4), 323–340. <https://doi.org/10.1177/13882627211031257>
152. van der Aalst, W. M. P., Bichler, M., & Heinzl, A. (2018). Robotic process automation. *Business & Information Systems Engineering*, 60(4), 269–272. <https://doi.org/10.1007/s12599-018-0542-4>
153. Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 22(4), 97–112. <https://doi.org/10.9785/cr-2021-220402>
154. Villani, C. (2018). *For a meaningful artificial intelligence: Towards a French and European strategy*. Mission assigned by the Prime Minister of France. <https://www.aiforhumanity.fr/>
155. 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>
156. Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*, 31(2), 841–887. <https://jolt.law.harvard.edu/assets/articlePDFs/v31/Cou nterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf>

157. Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems*, 12(4), 5–33.
<https://doi.org/10.1080/07421222.1996.11518099>
158. Willcocks, L., Lacity, M., & Craig, A. (2017). Robotic process automation: Strategic transformation lever for global business services? *Journal of Information Technology Teaching Cases*, 7(1), 17–28.
<https://doi.org/10.1057/s41266-016-0016-9>
159. Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*, 42(7), 596–615.
<https://doi.org/10.1080/01900692.2018.1498103>
160. World Economic Forum. (2023). *The future of jobs report* 2023.
<https://www.weforum.org/publications/the-future-of-jobs-report-2023/>
161. World Economic Forum. (2025). *The future of jobs report* 2025.
<https://www.weforum.org/publications/the-future-of-jobs-report-2025/>
162. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.