

WORKING PAPER

Artificial Intelligence Regulation in the Democratic Republic of the Congo

Designing a Rights-Based Governance Framework for the DRC and Central Africa

Mbuyu Bilga





WORKING PAPER

Artificial Intelligence Regulation in the Democratic Republic of the Congo

Designing a Rights-Based Governance Framework for the
DRC and Central Africa

Mbuyu Bilga

August 2026



Artificial Intelligence Regulation in the Democratic Republic of the Congo

Designing a Rights-Based Governance Framework for the DRC and Central Africa

Working Paper · August 2026

Author: Mbuyu Bilga

First published 2026

© 2026 Mbuyu Bilga. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the prior written permission of the author, except for brief quotations used in reviews, scholarly works, and other non-commercial uses permitted by copyright law.

The views and recommendations expressed in this working paper are those of the author. The proposed framework is a recommendation for legal and institutional design and does not constitute legal advice.

SUGGESTED CITATION

Bilga, M. (2026). *Artificial Intelligence Regulation in the Democratic Republic of the Congo: Designing a Rights-Based Governance Framework for the DRC and Central Africa*. Working Paper.

Table of Contents

	Abstract	iv
1	Introduction	1
2	Conceptualising Artificial Intelligence for Regulatory Purposes	3
3	Methodology and Scope	5
4	Constitutional Foundations of AI Governance in the DRC	6
5	The DRC Digital Code as the Immediate Legal Foundation	8
6	African and International Regulatory Context	9
7	The Regulatory Gap in the DRC	11
8	Proposed Congolese Artificial Intelligence Governance Framework	12
9	Institutional Architecture	16
10	Sector-Specific Applications	18
11	Liability and Accountability	19
12	Data Sovereignty and Cross-Border AI Services	20
13	Implementation Roadmap	20
14	Measuring Effectiveness Without Reducing Rights to Statistics	22
15	Anticipated Objections	23
16	Discussion: Toward a Congolese Model of AI Governance	24
17	Conclusion	25
	References	27
A	Appendix · Proposed minimum impact-assessment questions	28
B	Appendix · Proposed minimum contents of a public AI register	29
C	Appendix · Author's methodological disclosure	30

FIGURES AND TABLES

Fig. 1	The ten pillars of the proposed framework	13
Fig. 2	Phased implementation roadmap	22
Table 1	Regulatory categories and proportionate responses	4
Table 2	Proposed institutional architecture	17
Table 3	Minimum contents of a public AI register	29

Abstract

Artificial intelligence is moving from a predominantly private-sector technology to an infrastructure of public administration, commerce, security, education, health, media, and social decision-making. For the Democratic Republic of the Congo (DRC), this transition creates opportunities for public-service improvement and scientific development, but it also creates risks involving privacy, discrimination, opaque automated decisions, surveillance, cybersecurity, exclusion, linguistic inequality, labour disruption, and the transfer of sensitive data beyond Congolese control. The DRC already possesses a significant legal foundation through its Constitution and Ordinance-Law No. 23/010 of 13 March 2023 establishing the Digital Code. It also operates within a developing African and international governance environment shaped by the African Union Continental Artificial Intelligence Strategy, the African Union Convention on Cyber Security and Personal Data Protection, UNESCO's Recommendation on the Ethics of Artificial Intelligence, the OECD AI Principles, and comparative instruments such as the European Union AI Act. Yet a dedicated AI law should not be created by mechanically copying foreign legislation. This paper asks how the DRC can design a rights-based, risk-proportionate, institutionally feasible framework for artificial intelligence that is compatible with Congolese constitutional values, African priorities, and regional cooperation. Using doctrinal legal research, comparative analysis, and normative institutional design, the paper argues for a phased framework built around constitutional rights, lifecycle risk assessment, human responsibility, data governance, public-sector safeguards, algorithmic transparency, independent oversight, accessible remedies, public procurement controls, and regional interoperability. The paper proposes a Congolese Artificial Intelligence Governance Framework composed of ten pillars and recommends immediate rules for high-impact public and private uses, followed by institutional strengthening and sector-specific regulation. It concludes that the DRC should pursue **rights-based regulation before scale-based deployment**: the state should neither prohibit beneficial innovation nor permit unaccountable experimentation on the population. The appropriate model is a sovereign, African, multilingual, development-conscious, and legally enforceable system of trustworthy AI.

SECTION 1

1

Introduction

Artificial intelligence is no longer limited to research laboratories or technology companies. Machine-learning systems now classify images, generate text, recommend content, identify faces, detect fraud, translate languages, allocate attention, support medical decisions, assess creditworthiness, assist public authorities, and influence the information environments in which citizens form political and social judgments. The significance of AI therefore lies not only in the sophistication of software. It lies in the fact that automated systems increasingly participate in decisions that affect people's opportunities, identities, security, dignity, and access to public goods.

This development presents a specific regulatory challenge for the Democratic Republic of the Congo. The DRC is a large, diverse, multilingual, and constitutionally decentralized state whose digital transformation will occur under conditions that differ from those assumed by many high-income regulatory models. Digital infrastructure and public capacity are unevenly distributed. The Constitution recognizes French as the official language and identifies Kikongo, Lingala, Swahili, and Tshiluba as national languages, while also recognizing the wider linguistic heritage of the country.^[1] This linguistic reality matters for AI because models trained primarily on foreign or dominant-language data may perform poorly in Congolese contexts, may reproduce cultural and regional bias, and may exclude citizens from meaningful explanation or redress.

The DRC is not entering an empty legal space. Its Constitution establishes a rule-of-law state and protects equality, human dignity, freedom of expression, access to information, privacy, confidentiality of correspondence and telecommunications, and other rights that are directly relevant to automated decision-making.^[1] Ordinance-Law No. 23/010 of 13 March 2023, establishing the Digital Code, provides a broad legal architecture for digital activities and services, electronic tools, digital content, data protection, regulatory institutions, and cybersecurity.^[2] The Code creates or recognizes institutional functions that include an Authority for the Protection of Personal Data and a National Cybersecurity Agency.^[2] These provisions form a starting point for AI governance, even though a general-purpose AI system may create risks that were not fully anticipated when the Code was drafted.

At the continental level, the African Union adopted a Continental Artificial Intelligence Strategy in 2024. The official strategy presents an Africa-centric and development-focused approach that emphasizes ethical, responsible, and equitable AI and calls for unified national approaches, regional cooperation, and inclusive

development.^[3] The strategy is important because it rejects the assumption that African countries must simply import regulatory models designed elsewhere. At the same time, the African Union Convention on Cyber Security and Personal Data Protection—the Malabo Convention—provides a continental reference point for data protection and cybersecurity.^[4] Globally, UNESCO’s Recommendation on the Ethics of Artificial Intelligence identifies human dignity, human rights, proportionality, privacy, transparency, accountability, human oversight, sustainability, awareness, fairness, and non-discrimination as central principles.^[5] The OECD AI Principles similarly emphasize human rights and democratic values, transparency and explainability, robustness and safety, and accountability.^[6]

The European Union AI Act is another important comparative instrument. It adopts a risk-based architecture that distinguishes unacceptable-risk practices, high-risk systems, transparency obligations, and lower-risk uses.^[7] The Act is influential because it demonstrates how AI regulation can be translated from broad principles into duties, prohibitions, conformity requirements, institutional supervision, and sanctions. Yet the EU model cannot be transplanted without modification. The DRC has different state structures, administrative resources, language conditions, economic relationships, data ecosystems, and constitutional priorities. A law that copies the vocabulary of the EU while lacking feasible supervision could create symbolic regulation rather than effective protection.

A law that copies the vocabulary of the EU while lacking feasible supervision could create symbolic regulation rather than effective protection.

This paper therefore addresses the following research question: **How should the Democratic Republic of the Congo design a rights-based governance framework for artificial intelligence that protects constitutional rights, supports beneficial innovation, remains institutionally feasible, and is compatible with African and regional cooperation?** The paper advances three subsidiary questions. First, what legal resources already exist in Congolese constitutional and digital law? Second, what can the DRC learn from African, international, and comparative AI-governance instruments without copying them uncritically? Third, what institutional, procedural, and substantive safeguards should be adopted for AI systems used by government, businesses, courts, schools, health providers, employers, and security agencies?

The central argument is that the DRC should adopt a **phased, risk-based, rights-centred AI governance framework** rather than rely on either laissez-faire deployment or an immediately comprehensive statute that cannot be implemented. The framework should begin with high-impact uses, especially systems that affect public benefits, identity, policing, migration, employment, education, health, credit, justice, and access to essential services. It should require lawful

purpose, necessity, proportionality, data governance, human responsibility, impact assessment, transparency appropriate to the affected person, independent oversight, security, documentation, and accessible remedies. It should build on the Digital Code instead of creating an isolated and contradictory regulatory regime.

The paper makes four contributions. First, it identifies AI governance as a constitutional issue rather than merely a technology-policy issue. Second, it develops a DRC-specific adaptation of risk-based regulation that recognizes linguistic diversity, limited regulatory capacity, public procurement dependence, and cross-border data flows. Third, it proposes an institutional design that distributes responsibilities among existing and new bodies while reducing fragmentation. Fourth, it presents an implementation roadmap that distinguishes immediate, medium-term, and long-term reforms.

The paper is a doctrinal and normative policy study. It does not claim to provide empirical measurements of AI adoption in the DRC, and it does not report interviews or surveys that have not been conducted. The proposed framework is therefore an argument for legal and institutional design, supported by primary legal texts and authoritative international instruments. Its recommendations should be tested through consultation with Congolese regulators, courts, civil society, technology professionals, universities, journalists, health authorities, businesses, and communities before enactment.

SECTION 2

2

Conceptualising Artificial Intelligence for Regulatory Purposes

A serious AI law must begin with a workable definition. Definitions that are too narrow become obsolete as technologies change. Definitions that are too broad may classify ordinary software as AI and impose disproportionate obligations. The regulatory question is not whether a system is marketed as “intelligent.” It is whether the system uses computational methods to generate outputs—such as predictions, recommendations, classifications, content, or decisions—that can influence physical or virtual environments and affect people or institutions.

For this paper, an **AI system** means a machine-based computational system that, for explicit or implicit objectives, infers from inputs how to generate outputs such as predictions, content, recommendations, classifications, or decisions that may influence physical or virtual environments. This functional definition is compatible with the direction of contemporary international instruments while allowing

national regulators to address emerging technologies without repeatedly amending the definition of AI.

The definition should be supplemented by categories that describe the system's function and risk. A large language model used to draft a private document is not equivalent to a biometric identification system used by law enforcement. A recommendation tool for entertainment is not equivalent to a system that ranks applicants for public employment. The same underlying model can be low-risk in one context and high-risk in another. Regulation should therefore focus on **use, impact, and power**, not only on technical architecture.

TABLE 1
Regulatory categories and proportionate responses

Regulatory category	Illustrative use	Principal concern	Appropriate response
 Minimal-risk	Spam filtering, accessibility tools, routine translation, personal productivity	Limited individual harm	Voluntary guidance, literacy, basic security
 Limited-risk	Chatbots, synthetic media, recommendation systems	Deception, confusion, manipulation	Notice, labelling, user controls, complaint channels
 High-impact	Employment, education admission, credit, insurance, health triage, essential services	Discrimination, exclusion, opacity	Impact assessment, documentation, human review, audit, remedy
 Rights-critical	Policing, biometric identification, migration, criminal justice, political processes	Liberty, privacy, equality, democratic integrity	Strict necessity and proportionality, independent authorization, heightened oversight
 Prohibited or presumptively prohibited	Social scoring, coercive manipulation, indiscriminate surveillance, systems designed to exploit vulnerability	Severe or systemic rights violations	Prohibition or narrowly defined exception subject to judicial control

This taxonomy should not be treated as fixed. The National AI Governance Council proposed below should maintain a public register and update technical guidance. However, changes to the category of a use that affects constitutional rights should not be left entirely to an administrative office without public consultation and judicial review.

AI risk also exists at different stages of the lifecycle. Data collection can create privacy and representational harm. Model training can encode bias or unlawful acquisition. Deployment can produce inaccurate or discriminatory outputs. Integration into an institution can remove meaningful human judgment. Post-deployment updates can alter performance without notice. Decommissioning can leave personal data, copied models, or automated decisions in circulation. A rights-

based law must therefore impose duties across the lifecycle rather than only at the point of sale.

SECTION 3

3

Methodology and Scope

This paper uses three methods. The first is **doctrinal legal analysis**. It examines the DRC Constitution and the Digital Code as the primary national foundations, then relates them to African and international instruments. The purpose is not to provide a complete commentary on every provision of the Digital Code. It is to identify rights, duties, institutions, and gaps that matter for AI.

The second method is **comparative legal analysis**. The paper examines the African Union Continental AI Strategy, the Malabo Convention, UNESCO's Recommendation, the OECD AI Principles, and the EU AI Act. These instruments are not treated as identical sources of law. Some are binding treaties, some are recommendations, some are strategies, and some are domestic or regional legislation. Their comparative value lies in the institutional choices and regulatory techniques they reveal.

The third method is **normative institutional design**. On the basis of the legal analysis, the paper develops a proposed framework for the DRC. The proposal is assessed using six criteria: rights protection, administrative feasibility, regulatory clarity, democratic accountability, innovation compatibility, and regional interoperability.

The paper has four limitations. First, the DRC's AI market, public-sector deployments, and private-sector practices require empirical study beyond the scope of this manuscript. Second, the Digital Code is a broad and developing instrument, and implementation practice may change over time. Third, comparative legal analysis cannot establish that a foreign model will work in the DRC. Fourth, the paper does not replace consultation with Congolese stakeholders or a formal legislative drafting process.

SECTION 4

4

Constitutional Foundations of AI Governance in the DRC

4.1 Rule of law and human dignity

The Constitution defines the DRC as a state based on the rule of law, democratic, social, and secular.^[1] It also places the individual under state protection and recognizes the right to life, physical integrity, and free development of personality.^[1] These provisions have direct implications for AI. Public authorities cannot treat automated systems as neutral instruments that remove the need for legal justification. When the state uses an AI system to classify, monitor, investigate, or decide, the legal basis and rights implications of that use remain attributable to the state.

Human dignity provides a substantive limit on the treatment of people as data points or risk scores. A person affected by an automated decision should not be reduced to an unexplained probability where the decision determines access to essential rights or services. Dignity requires that people remain visible as rights-holders capable of explanation, participation, challenge, and review.

4.2 Equality and non-discrimination

The Constitution recognizes equality before the law and equal protection, prohibits discrimination on grounds including origin, social condition, residence, political views, race, ethnicity, tribe, and cultural or linguistic minority, and requires public authorities to eliminate discrimination against women.^[1] These provisions are especially important in the DRC because AI systems can reproduce unequal patterns through training data, proxy variables, language performance, geographic underrepresentation, and unequal access to digital systems.

A rights-based AI law should therefore prohibit discriminatory outcomes and not merely discriminatory intentions. It should also recognize indirect discrimination. A system may appear to use neutral variables—such as location, language, device type, educational history, or communication patterns—but may produce exclusion correlated with ethnicity, gender, disability, poverty, or region. High-impact deployers should be required to assess disparate impacts before and during deployment and to provide accessible routes for individuals to challenge harmful results.

4.3 Freedom of expression and access to information

Article 23 of the Constitution protects freedom of expression, while Article 24 recognizes the right to information and protects the freedom of the press, information, and broadcasting.^[1] AI governance must protect these rights in at least four ways.

First, content moderation and automated filtering should not become invisible systems of censorship. Platforms and public authorities should provide reasons, notice, appeal, and human review where automated systems restrict access to lawful expression. Second, synthetic media and automated political content require transparency, but labelling rules should not be used to suppress criticism or journalism. Third, public-sector AI systems should be subject to transparency and access-to-information rules, subject to legitimate security and privacy exceptions. Fourth, AI literacy should enable citizens to understand how automated systems shape information environments.

4.4 Privacy and confidentiality of communications

Article 31 protects private life and the confidentiality of correspondence, telecommunications, and other forms of communication, permitting interference only in cases provided by law.^[1] AI systems can threaten privacy through biometric recognition, behavioural profiling, predictive analytics, voice processing, location tracking, scraping, and inference of sensitive characteristics from apparently ordinary data.

Privacy protection must therefore address both collected data and inferred data. A system may create sensitive information about a person without asking for a direct statement of that information. For example, it may infer health, political affiliation, religion, ethnicity, or emotional state. Congolese regulation should require a lawful basis, specified purpose, necessity, proportionality, data minimization, security, retention limits, and independent oversight for high-risk processing.

4.5 Language, inclusion, and national diversity

The constitutional recognition of French, four national languages, and the wider cultural heritage of other languages should inform AI policy.^[1] A system that works only in French may be formally available but practically inaccessible to citizens whose strongest language is Lingala, Swahili, Kikongo, Tshiluba, or another local language. This is not a simple technical inconvenience. It may affect access to public information, education, legal services, health advice, and remedies.

The framework proposed in this paper therefore treats language inclusion as a governance obligation. High-impact systems should disclose the languages in which they can operate reliably. Public authorities should not deploy a system for essential services without testing whether its performance is materially unequal

across relevant language groups. Where automated explanations cannot be provided in a person's effective language, a human channel must be available.

SECTION 5

5

The DRC Digital Code as the Immediate Legal Foundation

Ordinance-Law No. 23/010 of 13 March 2023 establishes the DRC Digital Code.^[2] The Code is structured around digital activities and services, electronic writings and tools, trust-service providers, digital content, personal data, cybersecurity, and institutional authorities.^[2] The existence of this broad framework is significant: the DRC need not begin AI governance by legislating from an institutional vacuum.

The Code contains a book on personal data and a title concerning an Authority for the Protection of Personal Data. The extracted text of the Code states that Article 262 creates an Authority for the Protection of Personal Data, known as the APD, charged with controlling compliance with the personal-data provisions and matters relating to privacy and foreign action affecting data or data processing.^[2] Article 263 assigns the Authority a mission to ensure that processing of public and personal data complies with the relevant provisions.^[2] The Code also provides for organs of the Authority and for administrative decisions and sanctions subject to legal challenge.^[2]

These provisions can support AI regulation in at least five ways. First, they provide a legal basis for regulating training data, inputs, outputs, and profiling where personal data are involved. Second, they create an institutional home for data-protection supervision. Third, they support rights of access, correction, opposition, and other data-subject protections described in the Code. Fourth, they connect data governance with cybersecurity. Fifth, they create a platform on which AI-specific duties can be added through legislation or regulation.

The Code also creates a National Cybersecurity Agency. Article 275 describes the National Cybersecurity Agency as a public body with legal personality and responsibility for cybersecurity and the security of information systems in the DRC.^[2] This is relevant because AI systems can be attacked through data poisoning, model manipulation, prompt injection, unauthorized access, extraction of personal information, and supply-chain vulnerabilities. AI governance cannot be separated from cybersecurity governance.

Nevertheless, the Digital Code does not automatically solve AI-specific problems. Traditional data-protection rules may not answer whether an automated public-benefit decision must be explained, whether a deployer may rely on a foreign foundation model, whether an employer may use emotion recognition, who bears liability for an autonomous system, or how a citizen challenges a machine-assisted decision. Data protection is necessary but not sufficient. The DRC requires an additional layer of AI-specific duties focused on impact, accountability, human oversight, and institutional use.

Data protection is necessary but not sufficient.

SECTION 6

6

African and International Regulatory Context

6.1 African Union Continental Artificial Intelligence Strategy

The African Union Continental Artificial Intelligence Strategy presents AI as an area requiring an Africa-centric, development-focused approach that is ethical, responsible, equitable, and coordinated.^[3] The strategy calls for unified national approaches among member states and stronger regional and global cooperation.^[3] Its importance for the DRC is both substantive and institutional.

Substantively, the strategy recognizes that AI should serve African priorities rather than only foreign commercial interests. This supports regulation that addresses language, infrastructure, digital skills, health, education, agriculture, public services, culture, and the risks of external dependence. Institutionally, the strategy supports cooperation on standards, data governance, capacity, research, and responsible innovation.

The DRC should use the continental strategy as a policy compass but translate its principles into enforceable national duties. A continental strategy cannot itself provide every individual with a remedy against a harmful automated decision. The national framework must specify which institution supervises, what the deployer must document, what the affected person can request, and which court or tribunal can provide relief.

6.2 The Malabo Convention

The African Union Convention on Cyber Security and Personal Data Protection establishes a continental framework for cybersecurity, electronic transactions, and

personal-data protection.^[4] Its significance is that AI systems depend on data and computational infrastructures whose risks cross borders. The DRC's AI framework should be compatible with continental data-protection and cybersecurity principles, particularly in relation to lawful processing, security, cooperation, and rights protection.

The Malabo Convention should not be read as eliminating the need for DRC-specific rules. It provides a baseline and a cooperation channel. The DRC still needs to decide how its national authority supervises AI systems, how public bodies perform impact assessments, how local languages are treated, and how individuals challenge decisions.

6.3 UNESCO Recommendation

UNESCO's Recommendation on the Ethics of Artificial Intelligence was adopted by the organization's 193 Member States in November 2021 and describes itself as a global standard on AI ethics.^[5] It places human dignity and human rights at the core of AI governance and identifies four values: respect for human dignity and human rights; just, peaceful, and interconnected societies; diversity and inclusion; and the protection of the environment and ecosystems.^[5]

Its ten principles are directly useful for the DRC: proportionality and do no harm; safety and security; privacy and data protection; multi-stakeholder and adaptive governance; responsibility and accountability; transparency and explainability; human oversight; sustainability; awareness and literacy; and fairness and non-discrimination.^[5] The proposed DRC framework adopts these principles but converts them into more specific legal mechanisms.

6.4 OECD AI Principles

The OECD AI Principles, adopted in 2019 and updated in 2024, are described by the OECD as the first intergovernmental standard on AI.^[6] They promote innovative and trustworthy AI that respects human rights and democratic values. The values-based principles cover inclusive growth and well-being; human rights and democratic values including fairness and privacy; transparency and explainability; robustness, security, and safety; and accountability.^[6]

The OECD framework is helpful for its clarity and flexibility, but it is not a complete legislative model for the DRC. The OECD's emphasis on innovation and interoperability must be adapted to a setting in which the principal risks may arise from imported systems, public procurement, weak bargaining power, limited technical capacity, and unequal language coverage. In the DRC, accountability must include the public authority that purchases or deploys a system, not only the developer.

6.5 The European Union AI Act

The EU AI Act establishes a risk-based framework for AI developers and deployers. [7] It identifies prohibited practices, high-risk systems, limited-risk transparency obligations, and lower-risk uses. The European Commission describes the Act as the first comprehensive legal framework on AI worldwide.[7]

The EU model provides several transferable regulatory techniques. These include risk classification, prohibited practices, duties for high-risk systems, transparency requirements, conformity assessment, post-market monitoring, regulatory authorities, and penalties. It also demonstrates the importance of clear institutional responsibility.

However, the EU model should not be copied word-for-word in the DRC. The Act is lengthy, technically complex, and supported by extensive administrative, market, standardization, and enforcement capacity. A Congolese system should be more phased and should prioritize uses with direct effects on rights. It should also address the reality that many systems used in the DRC may be imported, cloud-based, open-source, or procured by public bodies with limited ability to inspect the underlying model.

SECTION 7

7

The Regulatory Gap in the DRC

The DRC's current legal foundation leaves at least eight AI-specific gaps.

First, there is no single general framework that classifies AI uses by risk. Without classification, the same compliance burden may be applied to trivial and rights-critical systems, while high-impact uses may escape special scrutiny.

Second, the legal framework requires stronger rules on automated decision-making. Individuals need to know when an AI system materially contributed to a decision, obtain an understandable explanation, request human review, correct inaccurate data, and challenge the outcome.

Third, public-sector procurement is a major gap. A ministry or public agency may acquire an AI tool through a contract whose technical terms are inaccessible to citizens and regulators. Procurement rules should require impact assessment, documentation, audit access, data-localization or data-transfer safeguards where appropriate, security testing, termination rights, and remedies.

Fourth, institutional fragmentation may create weak accountability. The APD, National Cybersecurity Agency, telecommunications regulator, digital-develop-

ment institutions, sector regulators, courts, and ministries may all have partial responsibilities. A coordinating mechanism is needed without undermining the legal independence of existing authorities.

Fifth, the law should address foundation models and general-purpose AI. These systems can be integrated into multiple sectors, may be trained on data of uncertain provenance, and may generate inaccurate or harmful outputs. The DRC does not need to regulate every model in the same way, but it should impose disclosure, risk, security, and responsibility duties on providers and deployers that make such systems available for high-impact uses.

Sixth, there is a lack of explicit rules on algorithmic discrimination and language performance. Constitutional non-discrimination principles should be operationalized through testing, documentation, and remedies.

Seventh, the framework should address cross-border data and infrastructural dependence. AI services may process Congolese data on servers outside the DRC, under foreign law, with limited visibility into subcontractors. Cross-border processing should not be prohibited automatically, but high-risk transfers should require assessment, safeguards, and accountability.

Eighth, remedies need to be practical. A right exists in formal terms only if a person can discover that AI was used, understand the reason for an adverse outcome, file a complaint without excessive cost, obtain human review, and approach an independent authority or court.

SECTION 8

8

Proposed Congolese Artificial Intelligence Governance Framework

This paper proposes ten pillars.

FIGURE 1

The ten pillars of the proposed Congolese Artificial Intelligence Governance Framework**Pillar 1 Constitutional anchoring**

The statute should state that AI governance must respect the Constitution, international human-rights obligations applicable to the DRC, and the Digital Code. The law should expressly identify dignity, equality, privacy, expression, access to information, due process, non-discrimination, and human responsibility as governing principles.

This clause would prevent AI regulation from becoming a purely technocratic exercise. It would also guide courts when applying general rights to new technologies.

Pillar 2 Risk-based classification

The law should classify systems according to their likely impact, affected population, reversibility of harm, sensitivity of data, degree of state power, and possibility of human challenge. The categories should include prohibited or presumptively prohibited uses, high-impact uses, limited-risk uses, and minimal-risk uses.

High-impact uses should include systems that determine or materially influence eligibility for public benefits, education admission, employment, credit, insurance, health services, housing, migration status, policing, criminal justice, electoral processes, or access to essential public services. The list should be reviewable and expandable through regulation.

Pillar 3 Prohibited practices

The DRC should prohibit AI systems that are inherently incompatible with constitutional rights unless a narrow statutory exception is justified by necessity, proportionality, and independent authorization. Prohibited or presumptively prohibited practices should include social scoring by public authorities; manipulative

systems that exploit a person's vulnerability to cause serious harm; indiscriminate biometric mass surveillance; covert emotion recognition for consequential public decisions; and automated systems designed to discriminate against protected groups.

The statute should be cautious about absolute prohibitions that are difficult to define. Each prohibition should be accompanied by technical guidance, examples, and a lawful process for determining whether a system falls within it.

Pillar 4 Duties for high-impact systems

A deployer of a high-impact AI system should be required to conduct an impact assessment before deployment. The assessment should describe the purpose, data, affected groups, expected benefits, foreseeable harms, language performance, cybersecurity risks, human oversight, accuracy limitations, procurement chain, retention, cross-border transfers, and remedies.

The assessment should be proportionate but not merely a private internal document. A public authority should publish a summary, and the APD or relevant sector regulator should have access to the complete assessment. High-impact systems should also be entered into a public register containing the deployer, purpose, provider, affected sector, risk category, date of deployment, and contact point for complaints.

Pillar 5 Human responsibility and review

An institution should never avoid responsibility by stating that “the algorithm decided.” The public authority, company, hospital, school, employer, bank, or other deployer must remain legally responsible for the decision and for selecting an appropriate system.

Individuals affected by a high-impact automated decision should receive notice that AI materially contributed to the decision. They should be able to request a meaningful explanation, submit relevant information, obtain review by a competent human decision-maker, and challenge the final decision. Human review must have authority to change the outcome; a nominal review that simply confirms the machine's output is insufficient.

Pillar 6 Data governance and linguistic inclusion

AI data practices must comply with the Digital Code and constitutional privacy protections. The law should require lawful purpose, necessity, minimization, accuracy, retention limits, security, and controls on secondary use. Sensitive data and inferred sensitive characteristics should receive heightened protection.

For public services, deployers should document the languages and populations represented in the data and test for material performance disparities. A person should not be denied an essential service merely because the AI system performs

poorly in a national or local language. Human assistance should be available where language performance is inadequate.

Pillar 7 Transparency, documentation, and audit

Transparency should be calibrated to the audience. The public needs to know where high-impact systems are used and for what purpose. An affected individual needs an explanation of the decision and a route to challenge it. A regulator needs technical documentation, testing data, risk assessments, incident records, and audit access. A developer may need protection for legitimate trade secrets, but trade secrecy should not prevent accountability for rights violations.

Independent audits should examine accuracy, bias, security, explainability, data provenance, environmental impacts, and compliance with stated purpose. Auditors should be competent and independent, and public authorities should not rely exclusively on a provider's self-certification.

Pillar 8 Public-sector procurement and deployment

The state should lead by example. Before acquiring a high-impact AI system, a public body should identify the legal basis, define the purpose, assess alternatives, evaluate rights risks, consult the APD and relevant regulator, and ensure that the contract contains audit, security, incident reporting, data-use, subcontracting, and termination provisions.

Procurement should not award a contract merely because a vendor demonstrates technical sophistication. The government should ask whether the system is necessary, whether a less intrusive alternative exists, whether its performance has been tested in Congolese conditions, whether affected persons can obtain redress, and whether the state will retain sufficient control over data and system outputs.

Pillar 9 Independent oversight and remedies

The APD should have authority over personal-data aspects of AI, while a proposed National AI Governance Council should coordinate cross-sector standards and risk guidance. Sector regulators should retain authority over health, education, telecommunications, finance, employment, and justice within their mandates.

The Council should not become a political body that replaces independent regulators. Its functions should include coordination, standards, a register, guidance, public consultation, capacity building, and an annual report. Enforcement should remain subject to administrative and judicial review.

Individuals should be able to complain to the deployer, the APD, the relevant sector regulator, an ombuds institution where applicable, or a court. Remedies should include explanation, correction, human reconsideration, suspension, deletion where lawful, compensation, and injunctions against unlawful deployment.

Pillar 10 Innovation, research, and regional cooperation

Rights-based regulation should not prohibit universities, start-ups, civil society, or public agencies from experimenting with low-risk systems. The law should establish supervised regulatory sandboxes with clear limits, consent requirements, monitoring, and exit conditions. Sandboxes should not be used to waive fundamental rights.

The DRC should cooperate with the African Union, regional organizations, neighbouring states, universities, standards bodies, and civil society. Cooperation should focus on interoperable data protection, cybersecurity, cross-border investigations, professional training, language resources, safety testing, and shared research. Regional cooperation should strengthen Congolese capacity rather than create external control over national data or public decisions.

 SECTION 9**9****Institutional Architecture**

The proposed framework requires institutional clarity. The following model builds on existing authorities rather than creating a large number of overlapping bodies.

TABLE 2

Proposed institutional architecture

Institution	Principal responsibility	Safeguard against overreach
Ministry responsible for digital affairs	Policy, legislative coordination, national strategy	Parliamentary oversight and public consultation
Authority for the Protection of Personal Data	Data protection, privacy, data-processing investigations, data-subject rights	Legal independence, transparent appointments, judicial review
National Cybersecurity Agency	System security, incident response, resilience, technical standards	Separation from content control and political surveillance
National AI Governance Council	Coordination, risk guidance, public register, annual report, standards	Non-binding coordination where sector regulators have legal mandates
Sector regulators	Health, finance, education, telecoms, employment, justice, elections	Consistency with national AI principles and cross-agency reporting
Courts and administrative tribunals	Rights protection, review of sanctions, remedies	Reasoned decisions and access to technical expertise
Universities and accredited auditors	Independent testing, research, training, evaluation	Conflict-of-interest rules and transparent methodologies
Civil society and professional bodies	Public scrutiny, rights advocacy, consultation, literacy	Structured participation and access to information

The appointment process for oversight bodies is critical. A regulator formally independent but practically controlled by the executive will not provide meaningful protection in politically sensitive cases. Appointment criteria should include competence, integrity, gender and regional representation, conflict-of-interest restrictions, fixed terms, transparent removal procedures, budgetary safeguards, and parliamentary reporting.

The framework should also prevent the cybersecurity agency from becoming a general surveillance institution. Cybersecurity is essential, but security mandates must have legal limits, authorization requirements, data minimization, retention rules, and independent oversight. The state should not use the language of cybersecurity to bypass privacy and expression protections.

 SECTION 10

10

Sector-Specific Applications

10.1 Public administration and social services

AI used to allocate benefits, assess eligibility, identify fraud, prioritize cases, or predict public-service demand can affect vulnerable people. Public authorities should publish the purpose and legal basis, conduct impact assessments, maintain human review, and provide reasons and appeal. A person should not lose an essential benefit solely because of an unverified automated inference.

10.2 Policing, security, and criminal justice

Security-related AI requires the strictest controls because the state has coercive power. Facial recognition, predictive policing, automated risk assessments, and investigative analytics can produce false positives, collective suspicion, and discriminatory surveillance. Use should require a clear legal basis, necessity, proportionality, independent authorization, accuracy controls, audit logs, retention limits, and judicial remedies. Indiscriminate biometric mass surveillance should be prohibited.

10.3 Health

AI-supported diagnosis, triage, and patient management may improve services but can also create medical harm. Providers should disclose when AI materially contributes to a clinical recommendation, preserve clinician responsibility, validate performance in local populations, protect health data, and provide human review. Patients should not be denied care because a system is unavailable or unreliable.

10.4 Education

Automated admissions, student-risk prediction, examination monitoring, and adaptive learning systems can reinforce inequalities. Schools and universities should assess disability, language, socioeconomic, gender, and regional impacts. Students should be able to contest important decisions and should not be subjected to invasive monitoring without lawful justification.

10.5 Employment and labour

Employers should not rely on opaque systems to screen or rank workers without notice and review. Emotion recognition and personality inference in employment should be prohibited or strictly restricted. Workers should receive information about consequential automated monitoring and have access to collective representation and remedies.

10.6 Finance and insurance

Automated scoring can exclude people whose data are incomplete or generated in informal settings. Providers should test for discriminatory proxies, explain adverse decisions, permit correction, and ensure that a human can review a contested outcome. The framework should regulate both traditional financial institutions and technology firms offering algorithmic risk assessment.

10.7 Media and political processes

Generative AI can produce synthetic content, impersonation, and automated influence. Regulation must protect the integrity of elections without giving authorities a general power to suppress criticism. Transparency, provenance, political-advertising disclosure, platform appeal, and narrowly defined prohibitions on impersonation and incitement are preferable to vague bans on “false information.”

SECTION 11

11

Liability and Accountability

AI liability should be distributed according to control and preventability. A developer that knowingly supplies a defective system, a deployer that ignores warnings, a public authority that uses a system without legal basis, and a professional who blindly follows an output should not automatically receive the same legal treatment.

The law should recognize at least four forms of accountability. **Administrative accountability** concerns compliance, registration, assessment, reporting, and sanctions. **Civil accountability** concerns compensation for unlawful or negligent harm. **Criminal accountability** should apply where existing offences or new offences cover intentional misuse, unlawful processing, serious fraud, or deliberate

discriminatory deployment. **Constitutional and judicial accountability** concerns the review of state action and protection of fundamental rights.

The opacity of AI should not make proof impossible. In high-impact cases, deployers should preserve logs, documentation, decision records, and relevant data. Where a person demonstrates that a high-impact system materially affected a decision and the deployer fails to produce required records, courts should be able to draw appropriate evidentiary inferences subject to procedural fairness.

SECTION 12

12

Data Sovereignty and Cross-Border AI Services

AI systems often depend on international cloud infrastructure, foreign models, imported applications, and cross-border technical support. A rigid requirement that all data remain physically inside the DRC may be difficult to implement and may encourage false compliance. The better approach is risk-based control.

Low-risk processing may occur across borders under contractual and technical safeguards. High-risk processing should require a transfer assessment, clear purpose, security controls, limitations on onward transfer, incident reporting, and a responsible entity within the DRC. Sensitive public-sector and health data should receive heightened controls. The state should know where data are processed, who can access them, how long they are retained, and what happens when a contract ends.

Sovereignty also concerns computational and institutional dependence. If public authorities cannot inspect, audit, or challenge a system because the provider is foreign, the DRC may have formal sovereignty but little practical control. Procurement rules should require meaningful access to documentation, performance evidence, audit cooperation, and continuity plans.

SECTION 13

13

Implementation Roadmap

A realistic framework should be phased.

Phase I Foundation, 0–18 months

The government should establish an interministerial and multi-stakeholder working group; complete an inventory of public-sector AI systems; identify high-risk deployments; publish interim guidance for government procurement; appoint or strengthen the APD; develop AI literacy and judicial training; and begin consultations in French and national languages.

During this phase, public bodies should not deploy new high-impact systems without a legal-basis review, impact assessment, human-review procedure, and minimum documentation. A temporary register of public-sector AI systems should be created.

Phase II Framework legislation, 18–36 months

Parliament should adopt an AI Governance Law or amendments to the Digital Code. The law should define AI, classify risk, prohibit severe practices, regulate high-impact systems, establish duties for providers and deployers, provide rights of explanation and review, regulate procurement, and clarify institutional competence.

The drafting process should include public hearings, technical consultations, universities, civil society, the judiciary, sector regulators, business associations, women's organizations, disability organizations, and representatives of linguistic communities. A law drafted without affected communities may reproduce the exclusion it claims to prevent.

Phase III Sectoral regulation, 36–60 months

Sector regulators should issue rules for health, education, finance, employment, elections, media, justice, and security. Each sector should identify prohibited, high-impact, and lower-risk uses. Supervisory expertise and accredited auditors should be developed progressively.

Phase IV Regional interoperability and evaluation, after 60 months

The DRC should seek compatibility with African Union standards and regional cooperation mechanisms. It should publish annual reports on AI incidents, complaints, audits, language performance, enforcement, public procurement, and rights impacts. The framework should be reviewed periodically because technology and risks will evolve.

FIGURE 2
Phased implementation roadmap

PHASE I	PHASE II	PHASE III	PHASE IV
0–18 MONTHS Foundation	18–36 MONTHS Framework legislation	36–60 MONTHS Sectoral regulation	AFTER 60 MONTHS Regional interoperability and evaluation
• Interministerial and multi-stakeholder working group • Inventory of public-sector AI systems • Interim guidance for government procurement • AI literacy and judicial training	• AI Governance Law or amendments to the Digital Code • Rights of explanation and review • Public hearings and technical consultations	• Rules for health, education, finance, employment, elections, media, justice, and security • Accredited auditors developed progressively	• Compatibility with African Union standards • Annual reports on incidents, complaints, audits, and rights impacts

SECTION 14

14

Measuring Effectiveness Without Reducing Rights to Statistics

AI governance should be evaluated, but numerical indicators should not replace legal judgment. Useful indicators include the number of high-impact systems registered; the proportion with completed impact assessments; complaints received and resolved; average time to human review; discriminatory performance findings; security incidents; public-sector procurement compliance; availability of explanations in relevant languages; and enforcement outcomes.

However, a low number of complaints may indicate either low harm or lack of awareness and access. A high number of audits may indicate strong supervision or widespread non-compliance. Indicators must therefore be interpreted with qualitative evidence and independent review.

The National AI Governance Council should publish an annual **State of AI Rights in the DRC Report** containing both quantitative data and case narratives. The report should identify systems that were suspended, corrected, or withdrawn and should explain how affected persons obtained remedies. Transparency should include failure, not only innovation.

SECTION 15

15

Anticipated Objections

Objection 1 The DRC should wait until AI adoption is larger

Waiting may appear rational, but regulation is most effective before high-impact systems become entrenched. Procurement decisions, data infrastructures, and institutional practices can create irreversible dependencies. A proportionate framework can regulate high-risk uses without obstructing low-risk experimentation.

Objection 2 AI regulation will discourage investment

Unclear rules can discourage responsible investment more than clear rules. Providers that cannot meet basic safety, transparency, data, and remedy obligations should not gain a competitive advantage through externalizing harm. A phased framework can reduce compliance costs for low-risk systems while imposing stronger duties where consequences are serious.

Objection 3 The DRC lacks technical capacity

Capacity limitations are real, but they strengthen the case for prioritization, cooperation, universities, professional training, and independent audit. They do not justify allowing foreign vendors or public authorities to deploy systems without accountability. The framework should begin with a manageable number of high-impact uses and expand as expertise grows.

Objection 4 Human rights principles are too abstract

Human-rights principles become operational when connected to procedures. Privacy becomes purpose limitation, data minimization, security, and remedy. Equality becomes impact testing and anti-discrimination duties. Due process becomes notice, explanation, human review, and appeal. Dignity becomes a prohibition on treating individuals as unchallengeable scores.

Objection 5 Regulation will prevent African innovation

A rights-based model can support African innovation by creating trust, public legitimacy, research standards, and predictable rules. The relevant choice is not

regulation versus innovation. It is accountable innovation versus innovation that transfers risks to populations with limited ability to challenge it.

The relevant choice is not regulation versus innovation. It is accountable innovation versus innovation that transfers risks to populations with limited ability to challenge it.

SECTION 16

16

Discussion: Toward a Congolese Model of AI Governance

The proposed model differs from both unregulated deployment and the direct transplantation of the EU AI Act. It treats constitutional rights as the foundation, the Digital Code as the immediate legal infrastructure, the African Union strategy as a continental policy reference, and comparative instruments as sources of regulatory technique rather than ready-made law.

The model is **rights-based** because it begins with the person affected by the system, not merely with the provider's technical obligations. It is **risk-based** because it does not impose the same duties on every application. It is **phased** because institutional capacity must be built progressively. It is **African** because it addresses language, inclusion, sovereignty, capacity, and continental cooperation. It is **Congolese** because it is anchored in the Constitution, the Digital Code, national institutions, and the realities of the DRC. It is **development-conscious** because it permits beneficial innovation while refusing to define development as the absence of rights protection.

The most important institutional choice is to allocate responsibility to deployers, especially public authorities. A foreign provider may design a system, but the Congolese institution that uses it to determine a citizen's eligibility, liberty, employment, education, health, or security has exercised public or institutional power. It must therefore remain accountable. Outsourcing technology cannot mean outsourcing constitutional responsibility.

Outsourcing technology cannot mean outsourcing constitutional responsibility.

The most important substantive choice is to require meaningful human review. Human involvement is not automatically protective. A human who cannot understand the system, lacks authority to change the result, or is pressured to approve every output does not provide effective oversight. Human review must be competent, independent enough to question the output, and able to provide a reasoned alternative decision.

The most important inclusion choice is language. An AI framework that operates only in elite or foreign languages can reproduce a hierarchy of access. Linguistic inclusion should be treated as a quality, equality, and rights issue. The state should encourage investment in Congolese-language datasets, evaluation benchmarks, translation tools, speech technologies, and research partnerships, while protecting communities from extractive data collection.

Finally, the DRC should avoid a regulatory model that emphasizes declarations without enforcement. A framework with many principles but no register, no audits, no records, no complaints, no remedies, and no budget will not protect anyone. The paper's proposed pillars are therefore designed to connect principle to institution and institution to procedure.

SECTION 17

17

Conclusion

Artificial intelligence will affect the DRC not only through future domestic laboratories but through imported applications, cloud services, public procurement, telecommunications, health systems, education platforms, financial products, media systems, security tools, and administrative decisions. The question is therefore not whether the DRC should regulate AI. It is whether it will regulate AI before powerful systems become embedded without transparency or accountability.

The DRC already has important foundations. Its Constitution protects dignity, equality, expression, information, privacy, and confidentiality. Ordinance-Law No. 23/010 establishes a Digital Code covering digital services, data protection, cybersecurity, and relevant authorities. The African Union Continental AI Strategy provides a continental direction that is ethical, responsible, equitable, and Africa-centric. UNESCO and OECD instruments provide widely recognized rights-based principles, while the EU AI Act demonstrates how risk classification can be translated into enforceable duties.

These instruments should inform but not dictate the Congolese model. The DRC should not copy foreign legislation without regard to its constitutional order, administrative capacity, linguistic diversity, regional structure, and data realities.

It should instead adopt a phased framework with ten pillars: constitutional anchoring; risk classification; prohibited practices; high-impact duties; human responsibility and review; data and language governance; transparency and audit; public procurement safeguards; independent oversight and remedies; and innovation and regional cooperation.

The proposed thesis is straightforward: **the DRC should pursue rights-based regulation before large-scale AI deployment.** It should enable beneficial systems while preventing technologies that undermine dignity, equality, privacy, liberty, democratic participation, or public accountability. A successful Congolese AI framework will not be measured by the number of systems deployed or the sophistication of imported tools. It will be measured by whether people can understand, challenge, and obtain remedy for automated power exercised over their lives.

The DRC has an opportunity to participate in the formation of African AI governance rather than merely receive rules created elsewhere. Its contribution can be a model that treats technological progress and human rights as mutually necessary. The future of AI in the DRC should therefore be sovereign without being isolated, innovative without being reckless, African without being exclusionary, and digital without ceasing to be human.

SOURCES

References

1. Constitution of the Democratic Republic of the Congo, 2005 (promulgated Feb. 18, 2006; revised by Law No. 11/002 of Jan. 20, 2011). [Online]. Available: <https://constitutionnet.org/sites/default/files/DRC%20-%20Congo%20Constitution.pdf>

2. Democratic Republic of the Congo, *Ordonnance-loi n° 23/010 du 13 mars 2023 portant Code du numérique*, Kinshasa, Mar. 13, 2023. [Online]. Available: <https://www.refworld.org/legal/natleginstr/natlegbod/2023/150225>. Supplementary text and structure: <https://droitnumerique.cd/code-du-numerique-congolais-rdc-pdf/>

3. African Union Commission, *Continental Artificial Intelligence Strategy*. Addis Ababa, Ethiopia: African Union, 2024. [Online]. Available: <https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy>

4. African Union, *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention), Malabo, Equatorial Guinea, Jun. 27, 2014. [Online]. Available: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

5. UNESCO, *Recommendation on the Ethics of Artificial Intelligence*. Paris, France: UNESCO, 2021. [Online]. Available: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

6. OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, adopted May 22, 2019, amended May 3, 2024. [Online]. Available: <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449>. See also OECD, “AI principles”: <https://www.oecd.org/en/topics/sub-issues/ai-principles.html>

7. 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), *Off. J. Eur. Union*, L series, Jul. 12, 2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>. See also European Commission, “AI Act”: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Further reading

OECD, “AI governance in Africa: Insights from a policy dialogue with 12 countries,” *OECD Artificial Intelligence Case Studies*. Paris, France: OECD Publishing, 2026. [Online]. Available: https://www.oecd.org/en/publications/oecd-artificial-intelligence-case-studies_c517cf5-en/ai-governance-in-africa_1ff55135-en.html

Organisation of African Unity, *African Charter on Human and Peoples’ Rights*, Nairobi, Kenya, Jun. 27, 1981. [Online]. Available: <https://achpr.au.int/en/node/873>

United Nations General Assembly, *International Covenant on Civil and Political Rights*, Dec. 16, 1966. [Online]. Available: <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

United Nations General Assembly, *Universal Declaration of Human Rights*, Res. 217 A (III), Dec. 10, 1948. [Online]. Available: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

 APPENDIX

A

Proposed minimum impact-assessment questions

- | | |
|-----------|--|
| 01 | What precise problem is the AI system intended to address, and is the purpose lawful? |
| 02 | What less intrusive alternatives were considered? |
| 03 | Which individuals, groups, communities, and languages may be affected? |
| 04 | What data are collected, inferred, retained, transferred, or reused? |
| 05 | What evidence supports accuracy, reliability, security, and performance in Congolese conditions? |
| 06 | What risks of discrimination arise by region, gender, disability, language, age, ethnicity, or socioeconomic status? |
| 07 | What happens when the system is uncertain, unavailable, manipulated, or wrong? |
| 08 | Who is legally responsible for the output and final decision? |
| 09 | How will an affected person receive notice, explanation, human review, correction, and appeal? |
| 10 | What independent audit, monitoring, incident-reporting, and suspension procedures exist? |
| 11 | What contractual rights does the DRC retain over data, logs, models, updates, and termination? |
| 12 | How will the system be evaluated after deployment, and under what conditions will it be withdrawn? |
-

APPENDIX

B

Proposed minimum contents of a public AI register

TABLE 3
Minimum contents of a public AI register

Field	Required information
Deploying institution	Name and responsible office
Provider	Legal identity, country, subcontractors
Purpose	The decision, service, or function supported
Risk category	Minimal, limited, high-impact, or prohibited review
Affected persons	Population and sector
Data	Categories, sources, retention, transfers
Languages	Languages supported and tested
Human oversight	Responsible official and review process
Assessment	Date and summary of impact assessment
Audit	Auditor, date, scope, principal findings
Incidents	Material errors, breaches, complaints, suspensions
Remedy	Contact point and appeal route

C

Author's methodological disclosure

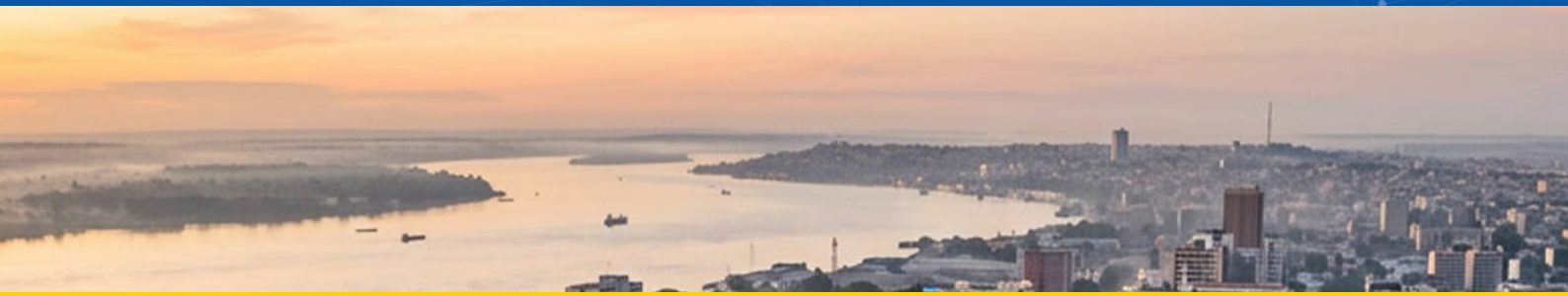
This manuscript is a doctrinal, comparative, and normative working paper. It does not present original survey data, interviews, experiments, or statistical estimates. Claims about the DRC legal framework are based on the cited constitutional and Digital Code sources. Comparative claims are based on the cited official African Union, UNESCO, OECD, and European Union materials. The proposed institutional framework is the author's recommendation and should be evaluated through Congolese legislative consultation, stakeholder research, and empirical study before adoption.

Rights-based regulation before **scale-based deployment**

Artificial intelligence is moving from a predominantly private-sector technology to an infrastructure of public administration, commerce, security, education, health, media, and social decision-making.

This paper asks how the DRC can design a rights-based, risk-proportionate, institutionally feasible framework for artificial intelligence that is compatible with Congolese constitutional values, African priorities, and regional cooperation.

The paper proposes a Congolese Artificial Intelligence Governance Framework composed of ten pillars and recommends immediate rules for high-impact public and private uses, followed by institutional strengthening and sector-specific regulation.



The future of AI in the DRC should therefore be sovereign without being isolated, innovative without being reckless, African without being exclusionary, and digital without ceasing to be human.