JOURNAL OF ARTIFICIAL INTELLIGENCE AND ROBOTICS
Apr-Jun 2025, VOL. 2, ISSUE 2, pp. 25-39
https://doi.org/10.61577/jaiar.2025.100008

RESEAPRO JOURNALS

REVIEW

OPEN ACCESS

Statutory, institutional, and policy reforms for a contextualised AI legal framework in West Africa's renewable-energy sector

Monday Clement Udoh

Department of Law, University of Calabar, Calabar, Nigeria

ABSTRACT

Machine learning is rapidly reshaping West Africa's renewable-energy sector, offering advanced forecasting, grid optimisation, predictive maintenance, and distributed energy management. Yet, regulatory frameworks lag behind technological deployment, leaving oversight weak, accountability fragmented, and public protections underdeveloped. Unlike the European Union, which implements the Artificial Intelligence Act, West Africa lacks coherent statutory, institutional, and regional governance mechanisms. This paper proposes a multi-dimensional reform roadmap for ECOWAS member states, addressing statutory authorization, institutional capacity, regional coordination, procedural safeguards, and ethical obligations. It advocates a Regional Registry of High-Risk AI Systems to track cross-border deployment, support coordinated incident response, and enhance transparency and procurement fairness. Mutual recognition of AI certifications is recommended to harmonize standards, reduce vendor compliance burdens, and prevent regulatory arbitrage, thereby securing energy infrastructure while fostering regional integration under the West African Power Pool. Capacity building is positioned as a core regulatory safeguard. The framework distinguishes general AI literacy from machine-learning oversight competence, establishes minimum skill thresholds for regulators and judicial actors, and proposes phased, measurable targets for operational and regional technical capacity. Socio-technical rights are embedded into governance, operationalizing equality, privacy, procedural justice, and socio-economic protections in energy allocation and service delivery. AI-specific cybersecurity risks including data poisoning, adversarial attacks, and model theft, are addressed through tailored safeguards and institutional coordination. Procurement reforms balance enforceable obligations with aspirational goals, promoting transparency, interoperability, and local innovation while preventing dependency on foreign systems. By linking technical, legal, institutional, and socio-ethical dimensions, this paper provides a context-sensitive, actionable framework for sustainable, equitable, and accountable AI deployment in West Africa's renewable-energy infrastructure.

KEY WORDS

Nanorobots; Artificial intelligence (AI); Drug delivery; Healthcare monitoring

ARTICLE HISTORY

Received 28 April 2025;
Revised 19 May 2025;
Accepted 30 May 2025

Introduction

Artificial intelligence is changing the global energy sector fast. It's unlocking new ways to forecast demand, balance grids, predict outages, and manage distributed energy. In West Africa, the story's no different. Here, donor-backed mini-grids, regional market software, predictive maintenance tools, and smart distribution systems are rolling out across the region. But this wave of digital innovation comes with a catch there's almost no solid legal framework in place, no real oversight, and few protections to keep people safe or hold anyone accountable. The European Union has tackled AI regulation head-on with its comprehensive Artificial Intelligence Act. In contrast, West Africa's regulatory systems lag behind fragmented, outdated, not keeping pace with technology. This paper lays out a clear reform plan for ECOWAS member states, covering statutory, institutional, regional, procedural, and ethical dimensions. The goal is simple: help West Africa build strong legal frameworks for using AI in critical energy infrastructure.

Statutory and Regulatory Reform: Building a Legal Foundation for AI in Energy

The urgent need for binding AI legislation

Right now, AI systems are active in West African energy markets, but there's no clear legal authority backing them up. That goes against basic administrative-law principles public powers need a solid legal foundation, not just a technological push. This isn't some fringe idea; it sits at the core of both common-law and African legal traditions. In R v Secretary of State for the Home Department, exparte Fire Brigades Union, the House of Lords held that government action inconsistent with statutory intent is unlawful. Similarly, the Supreme Court of Nigeria in A.G. Bendel State v Aideyan confirmed that public bodies can only act within the scope of powers expressly conferred upon them. Where energy regulators approve or rely on AI systems without statutory grounding, they risk judicial invalidation for ultra vires action, breach of procedural fairness, and violation of due-process norms. This expose, without clear laws backing them up, regulators in the energy sector run into trouble when they start using artificial intelligence. Relying on automated systems without explicit support in legislation puts them on shaky legal ground. They risk stepping beyond what the law actually allows, which threatens both administrative legality and due process. This concern aligns with widely recognized administrative-law principles requiring that public bodies exercise their powers transparently, rationally, and in accordance with statutory limits [1].

Many AI systems operate as "black boxes." Relying on them without solid legal safeguards erodes accountability and

***Correspondence:** Mr. Monday Clement Udoh, Department of Law, University of Calabar, Calabar, Nigeria, e-mail: mondayclementudoh768@gmail.com

undermines the basic expectation that decision-makers should be able to justify their actions (Baldwin, Cave, & Lodge, 2012) [2]. For consumers, this can lead to various issues errors from algorithms, unequal access to services, and threats to privacy. Lack of transparency in data practices and minimal procedural protections only exacerbate these problems. These concerns are not isolated; they reflect a broader discussion in contemporary AI governance research, which repeatedly highlights the risks of using systems with little transparency and inadequate oversight [3].

Operators often face a maze of unclear liability rules. Without clear laws, no one really knows who's responsible if a technical glitch, a cybersecurity breach, or a flawed algorithm causes harm. This isn't just a technicality; it's a bigger problem in governance. We have seen in the research how states with weak regulatory systems struggle to get a grip on fast-moving tech like this [4]. Now, if you add AI to national energy grids without any standards for cybersecurity, safety, or reliability, things get riskier fast. Lax regulation opens the door to hackers, bad energy forecasts, and shaky infrastructure. These aren't just abstract threats. They chip away at trust in regulators and put national resilience on the line [3]. So, every ECOWAS country needs to pass a comprehensive Artificial Intelligence in Critical Infrastructure Act. This law should spell out what counts as an "AI system," "high-risk AI," "automated decision," and "critical energy infrastructure." All AI used in energy management? Label it high-risk. Make licensing mandatory. Build in strict rules for conformity assessments and certification. The law needs to insist on transparency, explainability, and real human oversight. It must also cover data governance, privacy, and cybersecurity. And when companies break the rules, there should be real consequences administrative, civil, and criminal.

Here's what a straightforward clause might look like: "No artificial intelligence system shall be deployed for the management, forecasting, optimisation, or operational control of any electricity-generation, transmission, or distribution infrastructure without prior certification from the National Artificial Intelligence Oversight Authority pursuant to this Act." This clause reflects the precautionary legal culture now adopted globally for AI in essential services.

Statutory and regulatory reform: Contextualizing machine-learning governance in the renewable-energy sector

This section maintains that statutory authorization is a necessary condition for the lawful deployment of machine-learning systems in West Africa's renewable-energy sector. From an administrative-law perspective, the absence of legislative grounding risks ultra vires delegation, procedural unfairness, and accountability deficits, particularly where algorithmic outputs materially influence regulatory or distributive decisions [5,6].

However, regulatory effectiveness requires moving beyond abstract references to "AI systems" and recognizing the technological diversity of machine-learning applications deployed in energy governance. Legal risks vary significantly depending on system function, learning dynamics, and degree of autonomy an observation increasingly reflected in comparative AI governance scholarship [7,8].

Differentiating classes of machine-learning systems in renewable energy

Machine-learning applications in renewable-energy systems can be broadly categorized into functionally distinct classes, each presenting specific legal and administrative challenges:

Forecasting and predictive models: These include load-forecasting models, wind-speed and solar-irradiance prediction systems, and climate-adjusted demand projections used for grid planning and tariff regulation. Such models are widely documented in energy-systems literature [9,10].

Legal risks:

- Opacity undermining the administrative duty to give reasons for decisions affecting rights or legitimate expectations
- Bias and representational gaps where historical data underrepresent rural or off-grid communities
- Data drift, particularly acute in climate-sensitive regions, leading to progressively unreliable regulatory decisions [11,12].

Optimization and allocation algorithms: These systems optimize grid dispatch, prioritize renewable-energy investments, or allocate subsidies and incentives. Optimization techniques are central to smart-grid governance and energy-market design [13].

Legal risks:

- Ultra vires decision-making, where algorithmic optimization effectively replaces statutorily mandated discretion.
- Indirect discrimination, as optimization objectives may encode efficiency criteria that systematically disadvantage marginalized regions.
- Reduced contestability, where affected stakeholders cannot meaningfully challenge algorithmically mediated outcomes [14].

Adaptive control and autonomous systems: These include self-learning control systems for smart grids, automated frequency regulation, and energy-storage management that retrain continuously on live data [15].

Legal risks:

- Dynamic delegation without renewed authorization, as retraining alters decision logic post-deployment.
- Attribution gaps, where no identifiable official retains effective control.
- Procedural instability, as evolving models undermine predictability a core requirement of the rule of law [16].

Translating administrative-law obligations into machine-learning system requirements

To avoid purely symbolic regulation, statutory reform must connect legal duties to concrete technical properties of machine-learning systems, an approach increasingly endorsed in AI governance frameworks [17,8].

Legality and scope of delegation: Statutes should specify whether learning systems are static or adaptive and define permissible retraining conditions. This mirrors emerging approaches in the EU AI Act, which differentiates risk and regulatory obligations based on system function and deployment context [18].

Procedural fairness and explainability: For forecasting and optimization models influencing regulatory decisions, the duty to give reasons should translate into model documentation, explainability mechanisms, and audit trails, proportionate to system complexity [19,20].

Accountability and human oversight: Administrative law

https://doi.org/10.61577/jaiar.2025.100008

requires identifiable responsibility. Statutory provisions should mandate human-in-the-loop or human-on-the-loop oversight, particularly for adaptive systems with real-time decision authority [6].

Data governance and drift management: Given the climatic volatility affecting renewable-energy systems in West Africa, statutes should require periodic validation, drift detection, and re-authorization of retrained models, aligning legal oversight with well-established machine-learning risk-management practices [12].

Implications for West Africa's Renewable-Energy Governance

By grounding statutory obligations in the operational realities of machine-learning systems, West African legislators can avoid both technological abstraction and regulatory inertia. A contextualized AI legal framework should therefore adopt function-specific statutory provisions, rather than a single undifferentiated definition of "AI". This approach aligns administrative-law principles legality, fairness, accountability, and reason-giving with the technical characteristics of machine-learning systems, supporting both regulatory legitimacy and sustainable energy innovation.

Contextualized risk classification for West Africa

The EU AI Act sets up a four-level risk system: unacceptable, high-risk, limited-risk, and minimal-risk. But not every region lines up neatly with these categories. Digital infrastructure varies a lot. What counts as moderate risk in Europe often jumps to high risk in West Africa. There, problems like poor data protection, shaky cybersecurity, unstable electricity, and not much oversight raise the stakes. Take smart meters: in places without strong privacy rules, these devices can spill personal details about people's lives, making them a high-risk tool. Forecasting algorithms? When grid data's patchy or incomplete as it often is they start to look risky too. And predictive-maintenance models become indispensable for old infrastructure, where missing a warning isn't just a mistake, it's a costly one.

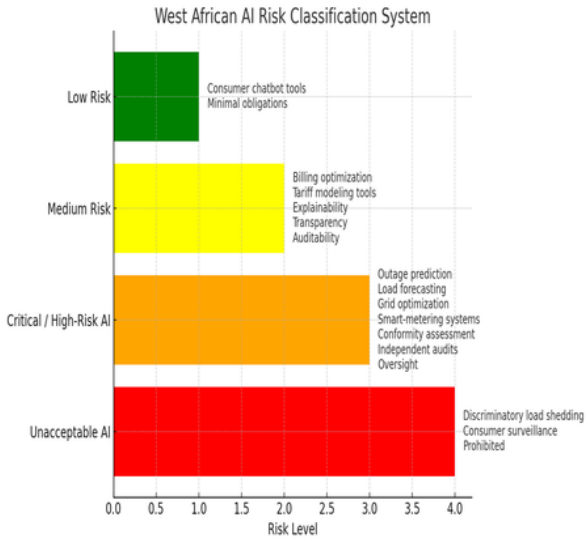

Figure 1. Proposed West African risk classification system.

This whole approach matches the rationality standard from the Wednesbury case [1]. Regulators need to make decisions that actually make sense in the messiness of the real world, not just on paper.

From Conceptual Taxonomies to Operational Criteria

The paper correctly rejects the uncritical transplantation of the EU AI Act's risk taxonomy into the West African renewable-energy context. As comparative regulatory scholarship cautions, risk classifications derive their legitimacy not merely from formal structure but from institutional capacity, infrastructural reliability, and data conditions [21,5]. In West Africa, infrastructure fragility, data sparsity, and uneven regulatory oversight substantially alter the real-world risk profile of machine-learning systems deployed in the energy sector.

However, to ensure regulatory practicability, contextualization must move beyond conceptual differentiation and articulate operational risk-classification criteria.

Risk dimensions and decision logic: A contextualized framework should classify AI systems along four cumulative dimensions, each tied to concrete system properties:

Decision Impact Severity

- Low: advisory forecasting tools without a binding regulatory effect.
- Medium: optimization systems influencing subsidy allocation or grid prioritization.
- High: adaptive control systems capable of autonomously altering grid operations [6].

Degree of Autonomy and Adaptivity

- Static models (no post-deployment learning).
- Periodically retrained models (batch updates subject to approval).
- Continuously learning systems (real-time adaptation) Continuous learning systems pose elevated rule-of-law risks due to evolving decision logic [12,15].

Data Robustness and Representativeness

- Availability of longitudinal, geographically representative datasets.
- Reliance on proxy or imported datasets due to local data scarcity. Dataset limitations significantly amplify bias and error risks in developing energy systems [22].

Institutional Capacity for Oversight

- Existence of technical audit capacity.
- Ability to suspend, override, or roll back systems. Where oversight capacity is weak, otherwise "moderate-risk" systems may warrant high-risk classification [21].

Contextual Risk Thresholds: Under this framework, an AI system should be classified as high-risk where any two of the following conditions are met:

- It materially affects access to electricity, tariffs, or subsidies.
- It operates with partial or full autonomy.
- It relies on non-representative or volatile datasets.

https://doi.org/10.61577/jaiar.2025.100008

- It is deployed in environments lacking real-time human oversight.

This cumulative logic avoids rigid taxonomies while preserving legal certainty and aligns risk classification with actual governance capacity rather than abstract technological labels.

Substantive Compliance Assessment: Embedding Machine-Learning Validation Practices

While this paper proposes a procedurally robust compliance framework, its regulatory effectiveness depends on integration with substantive machine-learning validation and monitoring practices. Without such integration, compliance risks devolving into a formal checklist rather than a meaningful safeguard, an outcome widely criticized in both AI governance and regulatory theory [23, 24].

Pre-Deployment Compliance Requirements: For medium- and high-risk systems, compliance assessments should mandate:

- **Performance Benchmarking**
  Models should be evaluated against baseline statistical or rule-based methods using sector-appropriate metrics (e.g., mean absolute percentage error for load forecasting), ensuring measurable performance gains [9].
- **Dataset Representativeness Audits**
  Developers must document data provenance, geographic coverage, and temporal relevance. Known dataset biases, especially urban overrepresentation, should be explicitly disclosed [22].
- **Model Documentation and Justification**
  Model cards or equivalent documentation should explain model purpose, limitations, and suitable deployment contexts [25].

Post-Deployment Monitoring and Drift Management: Given the climatic and infrastructural volatility of renewable-energy systems, compliance must extend beyond deployment:

- **Continuous Performance Monitoring**
  Regulators should require periodic re-evaluation against predefined performance thresholds, with mandatory reporting where degradation occurs [12].
- **Concept and Data Drift Detection**
  Systems should incorporate statistical drift detection or scheduled validation cycles, particularly where climate variability alters input distributions [11].
- **Model Update Governance**
  Retraining or architectural changes should trigger renewed compliance review for medium- and high-risk systems, preventing silent regulatory transformation [6].

Human Oversight and Accountability: Compliance regimes should require traceable human responsibility proportional to system autonomy. Adaptive control systems should be subject to human-on-the-loop oversight, including override and suspension powers, to preserve administrative accountability and procedural fairness [17].

Contribution to regulatory practicability

By embedding explicit risk criteria, cumulative thresholds, and machine-learning validation practices, this revised framework transforms contextualization from a normative aspiration into an operational governance tool. It preserves the paper's central claim that West Africa requires a locally grounded AI governance model while ensuring that risk classification and compliance function as substantive safeguards rather than symbolic procedures.

Mandatory conformity assessments prior to deployment

When AI runs energy systems, any failure can be catastrophic. That's why conformity assessment must be required before these systems go live, just as Article 43 of the EU AI Act demands. This follows the precautionary principle recognized in *Monsanto Agricoltura Italia SpA v Italy*.

Components of a West African conformity assessment framework

1. Safety Validation

- First, stress-test the system in simulated, real-world conditions.
- Run failure-mode analysis to see what happens when the AI makes a mistake.
- Test reliability during extreme weather (heatwaves, storms, droughts).

2. Data quality and integrity verification

- Check if the data represents both rural and urban areas fairly.
- Hunt for bias to prevent discrimination, as highlighted in *Enderby v Frenchay Health Authority*.
- Keep clear records of where the data comes from and how it's handled.

3. Cybersecurity Evaluation

- Do penetration testing and scan for vulnerabilities.
- Make sure data stays encrypted and travels securely.
- Assess how the system stands up to adversarial attacks.
- Mandatory incident-response procedures.

Institutional Reform: Building a Governance Architecture for AI Oversight

This section argues that effective governance of AI systems in West Africa's renewable-energy sector requires institutional independence, technical expertise, and specialized oversight capacity within energy regulators. Comparative experience from data protection, financial regulation, and energy-market governance supports the proposition that algorithmic decision-making cannot be effectively supervised through generalist administrative structures alone [6,21].

However, institutional legitimacy depends not only on normative desirability but also on feasibility, sequencing, and integration within existing governance ecosystems. In resource-constrained regulatory environments, the rapid creation of multiple high-capacity institutions risks fragmentation, duplication, and implementation failure [26].

Incremental institutional design rather than institutional proliferation

Rather than proposing the immediate establishment of fully autonomous AI supervisory authorities, this paper advocates an incremental, embedded oversight model that builds capacity within existing energy-regulatory institutions before

https://doi.org/10.61577/jaiar.2025.100008

progressing toward greater institutional differentiation. Comparative regulatory scholarship demonstrates that institutional the gradual addition of specialized functions within established regulators is more effective than wholesale institutional replacement, particularly in developing or transitional governance contexts [27].

Accordingly, AI oversight in the renewable-energy sector should initially be situated within:

- National electricity regulatory commissions
- Renewable-energy agencies
- Energy market operators

Specialized AI functions can be introduced as dedicated technical units, rather than standalone agencies, reducing startup costs and institutional resistance.

Functional differentiation within existing regulators

To balance feasibility and expertise, the section proposes functional differentiation, not institutional multiplication. Core oversight functions may be distributed as follows:

- **Technical Assessment Units**
  Small interdisciplinary teams (law, data science, energy systems) responsible for reviewing high-risk AI deployments, model documentation, and validation reports.
- **Audit and Inspection Functions**
  Existing compliance and inspection units can be extended to include algorithmic audits and performance reviews, drawing on established regulatory inspection powers.
- **Decision Accountability Structures**
  Final regulatory responsibility must remain with identifiable officials or boards, preserving administrative accountability and avoiding technocratic displacement [6].

This approach aligns with evidence that regulatory expertise is most sustainable when embedded in organizations with existing enforcement authority and sectoral knowledge [21].

Regional coordination and resource pooling

Given the shared infrastructural and data challenges across West Africa, regional coordination mechanisms offer a pragmatic solution to capacity constraints. Rather than duplicating high-cost technical expertise at the national level, states can pool resources through:

- Regional centres of excellence for AI and energy regulation
- Shared audit protocols and model evaluation standards
- Joint training and certification programmes for regulators

Such arrangements are consistent with regional regulatory cooperation models in energy and telecommunications and reduce both financial and technical barriers to effective oversight [28].

Transitional arrangements and capacity building

Effective institutional reform requires explicit transitional arrangements, particularly where AI systems are already in use. The paper therefore proposes a phased transition:

1. **Short-term (0–2 years)**
   - Designation of AI focal points within existing energy regulators
   - Mandatory registration of AI systems used in regulatory or grid operations
   - Reliance on external expertise (universities, development partners) for audits
2. **Medium-term (3–5 years)**
   - Establishment of permanent technical units
   - Development of internal audit capabilities
   - Gradual reduction of dependence on external consultants
3. **Long-term (5+ years)**
   - Possible evolution toward semi-autonomous AI oversight bodies, where justified by system maturity and deployment scale

Phased implementation reflects best practices in regulatory capacity building and avoids the legitimacy and effectiveness risks associated with premature institutional expansion [26].

Managing coordination and jurisdictional overlap

The introduction of AI oversight functions raises predictable coordination challenges with:

- Data protection authorities
- Competition regulators
- Cybersecurity agencies

Rather than creating rigid jurisdictional silos, the paper supports formal coordination mechanisms, such as memoranda of understanding, joint guidance, and shared audit triggers. Regulatory pluralism literature indicates that structured coordination is more effective than centralization in managing cross-cutting technological risks [21].

Preserving independence under resource constraints

Finally, institutional independence must be understood as functional independence, not necessarily full financial or organizational autonomy. Even within existing regulators, safeguards such as fixed terms for technical leads, transparent appointment criteria, and protected decision-making processes can meaningfully insulate AI oversight from political or commercial pressure [26].

Setting up “AI and Energy Safety Units” in energy commissions

Energy regulators cannot simply add AI oversight to existing portfolios; they require specialized AI-safety units. Recommended Expertise: Administrative and regulatory lawyers, Data scientists, System and electrical engineers, Cybersecurity specialists, Economists.

The Braganza duty essentially, the obligation to exercise discretion carefully and rationally demands that regulators really understand the technical systems they sign off on. Without that depth of knowledge, oversight becomes little more than a formality.

Technical collaboration with universities and research institutes

https://doi.org/10.61577/jaiar.2025.100008

Universities in West Africa can play several key roles. They can act as independent testing labs, partner with regulators on research, audit algorithmic fairness, and serve as hubs for AI and energy innovation. This approach follows the model of the EU's "Notified Bodies," which help regulatory agencies when they don't have the right specialists on hand.

Regional Harmonization Under Ecowas

Regional integration in accordance with ECOWAS: Enforcement capacity, differentiation, and dynamic governance.

This paper argues that regional integration under the auspices of ECOWAS is essential for governing AI systems deployed in West Africa's increasingly interconnected renewable-energy sector. Cross-border electricity trade, regional power pools, and shared digital infrastructure amplify systemic AI risks, including cascading failures, regulatory arbitrage, and accountability diffusion. In this respect, the paper correctly identifies regional coordination not as a normative aspiration but as a functional necessity.

However, effective regional integration requires a governance model that reflects ECOWAS's distinct institutional capacities, enforcement mechanisms, and member-state diversity, rather than assuming the transferability of EU regulatory templates.

ECOWAS integration beyond EU analogies

While the EU provides a useful reference point for regional AI governance, its institutional features direct effect of regulations, supranational enforcement bodies, and mature judicial integration are not mirrored within ECOWAS. ECOWAS integration relies predominantly on directives, coordination, and national implementation, with limited centralized enforcement capacity.

Accordingly, the proposed ECOWAS AI governance framework should be understood as coordination-oriented rather than command-and-control, aligning with existing ECOWAS energy and infrastructure instruments such as the ECOWAS Regional Electricity Regulatory Authority (ERERA) and the West African Power Pool (WAPP).

Enforcement capacity and differentiated obligations

Given disparities in regulatory maturity, grid infrastructure, and technical expertise among ECOWAS member states, uniform compliance obligations may prove counterproductive. The paper therefore supports a differentiated implementation model, under which:

- Core obligations (system registration, disclosure of high-risk AI use) apply uniformly
- Enhanced obligations (continuous monitoring, independent audits) apply only where national capacity exists
- Regional bodies provide technical support rather than punitive enforcement

Such differentiated integration is consistent with ECOWAS practice in energy and trade regulation and reflects broader scholarship on "variable geometry" in regional governance.

Regional registry as a living, dynamic infrastructure

The paper's proposal for a regional AI registry remains compelling but must account for the dynamic nature of machine-learning systems, particularly model updates, retraining, and performance drift.

Rather than a static database, the ECOWAS AI registry should operate as a living compliance infrastructure, requiring:

- **Event-based updates:** mandatory notification upon retraining, architectural modification, or dataset replacement
- **Periodic reaffirmation:** time-limited registrations (e.g., annual validity) for adaptive systems
- **Risk-tiered reporting:** higher reporting frequency for high-risk and adaptive systems

This approach aligns with established best practices in machine-learning governance, recognising that system risk evolves post-deployment [12,22].

Mutual recognition under conditions of ongoing validity

Mutual recognition of certifications is normatively attractive but technically fragile in the context of adaptive AI. To preserve regulatory credibility, recognition should be conditional and revocable, rather than permanent.

The paper therefore proposes conditional mutual recognition, whereby:

- Certifications are recognised only for a defined model version
- Substantial retraining triggers re-certification or notification
- Recognition is suspended where post-deployment monitoring reveals material performance degradation

This model avoids regulatory arbitrage while respecting national autonomy and limited enforcement resources, and it reflects lessons from cross-border conformity assessment regimes outside the EU.

Technical dispute resolution mechanisms

AI governance in a cross-border energy system will inevitably generate technical disputes, including:

- Conflicting model performance assessments
- Attribution of fault in cross-border grid failures
- Disagreements over compliance following system updates

Rather than relying exclusively on judicial mechanisms, which may lack technical capacity, the paper supports the establishment of expert-led regional technical panelsunder ECOWAS or ERERA auspices. Such panels could:

- Issue non-binding technical opinions
- Resolve disputes over model validation and drift
- Support harmonised interpretation of regional standards

Comparable expert-based dispute-resolution mechanisms are common in transnational energy governance and reduce both litigation costs and regulatory fragmentation.

Sustaining regional oversight over time

Finally, the paper emphasizes that regional AI governance must be adaptive rather than static. Periodic review of risk classifications, registry requirements, and certification criteria should be mandated at the regional level to reflect evolving machine-learning practices and infrastructural realities. This approach aligns with ECOWAS's incremental regulatory tradition and avoids overcommitment to prematurely rigid standards.

https://doi.org/10.61577/jaiar.2025.100008

ECOWAS regional registry of high-risk AI systems

ECOWAS needs a Regional Registry of High-Risk AI Systems. This isn't just a bureaucratic box to tick; it matters for all fifteen member states. With WAPP tying together energy transmission from country to country, a single AI-related incident in one place threatens the stability of the entire region. A shared registry does more than keep things transparent. It acts as a safeguard, helping every member state keep track of high-risk systems and respond before issues snowball.

Purpose and Rationale

A registry:

1. Improves regulatory oversight by providing an authoritative inventory of all AI systems deployed in generation, transmission, and distribution networks.
2. Strengthens cross-border risk management, ensuring that national regulators are aware of foreign-operated or vendor-managed systems influencing their grids.
3. Supports competition and procurement fairness by exposing vendor concentration, reducing monopolistic tendencies, and discouraging procurement opacity.
4. Enables coordinated responses to incidents, especially cyber events, technical failures, or discriminatory outcomes in load allocation.
5. Provides an evidentiary baseline for future litigation and judicial review, ensuring courts can assess the legality and scope of AI deployment when disputes arise.

The model is inspired by Article 60 of the EU AI Act, which set up a public database for high-risk AI systems. Adopting something similar in ECOWAS would open up the process, making it more transparent, while still keeping national security in mind.

Information Required for Registry Entry

Each member state would be required to submit detailed compliance documentation, including:

- full technical specifications of the AI system;
- the category of risk classification;
- conformity assessment reports;
- cybersecurity certification results;
- vendor and developer identification;
- jurisdiction and deployment environment;
- details of known failures, malfunctions, or bias incidents;
- human-oversight procedures and escalation pathways;
- data-governance structures, including location of data storage and processing.

Sensitive information, like infrastructure weaknesses, stays with authorized regulators. But non-sensitive details, such as who developed the system or its certification status, go public. This gives people more visibility and keeps everyone accountable.

Legal Basis within ECOWAS

The registry could be grounded in:

- ECOWAS Supplementary Act on Personal Data Protection, which already establishes regional cooperation mechanisms.
- ECOWAS Energy Protocol, recognizing the cross-border nature of energy infrastructure.
- Jurisprudence from the ECOWAS Court of Justice, which emphasises collective responsibility among member states in matters affecting regional welfare, as seen in *SERAP v Nigeria*.

This instrument would require a new supplementary act or directive to ensure enforceability across all ECOWAS jurisdictions.

Mutual recognition of AI certifications across member states

Mutual Recognition means that once an AI system gets certified in one ECOWAS country, every other state in the region accepts that certification. This approach cuts down on regulatory headaches and pushes everyone toward the same safety standards. Why does this matter? Mutual recognition smooths out the entire regulatory process. It keeps standards consistent and actually helps countries in the region work together especially when it comes to AI in essential infrastructure, like energy systems. Here's where mutual recognition really makes a difference: it speeds things up, keeps everyone on the same page, and strengthens regional cooperation.

Regional energy integration

The West African Power Pool (WAPP) is central to regional energy integration in West Africa. Making sure energy flows smoothly across borders isn't just an ambition it's essential. WAPP's mission goes beyond simply constructing lines or power plants; it strives for genuine coordination in how its member countries produce, transmit, and supply electricity. Picture an AI system managing load distribution in Ghana. The choices it makes affect not only Ghana's voltage and frequency stability, but also have impacts that reach Togo, Côte d'Ivoire, and Benin.

If every country insists on its own standards for certifying AI systems in the energy sector, complications arise. One country's certification process won't necessarily match another's. This lack of alignment leads to problems systems struggle to communicate, technical issues emerge, and the regional grid suffers. For example, an AI tool in Ghana used to predict energy loads might not be accepted in Togo if certifications aren't recognized, meaning it could fail or be unusable across the border. The consequences? Grids become unstable, power flows are interrupted, and energy supply is put at risk. This is why mutual recognition of AI system certifications is so important. It's not just bureaucracy. It is fundamental to keeping electricity flowing, grids reliable, and cross-border energy operations seamless. With a harmonized approach, WAPP can truly provide reliable, secure energy across the entire region.

Reduction of vendor compliance burden

Mutual recognition in AI regulation offers immediate, tangible benefits especially for vendors. Right now, they have to jump through hoops in every country, wrestling with different documentation rules, unpredictable certification processes, and conflicting data privacy laws. This patchwork drives up costs, slows down getting products to market, and makes it tough for new players to compete. Vendors end up tweaking

https://doi.org/10.61577/jaiar.2025.100008

their systems over and over to satisfy each country's standards. At the end of the day, innovation takes a back seat as companies pour resources into compliance. With mutual recognition, things change. When a country like Nigeria or Ghana certifies an AI system that meets the region's standards, every other member state recognizes that approval. The result? More consistency, less red tape, and lower compliance costs. Vendors can get their technologies out there faster and compete on a level playing field, which sparks more innovation throughout the sector.

Regulatory efficiency

Smaller ECOWAS countries often run up against the limits of their budgets and technical know-how when it comes to regulating high-risk AI systems. Building a solid certification process isn't easy when you're short on money and expertise especially if you're trying to keep up with the rapid pace of AI innovation in sectors like energy. Imagine a country with just a handful of regulators trying to evaluate a complex AI that manages its power grid. It's a tall order.

This is where mutual recognition of certifications makes a real difference. Instead of each country reinventing the wheel, they can count on larger players think Nigeria, Ghana, or Senegal to handle the heavy lifting on conformity assessments. If a high-risk AI system passes muster in one of these countries, others in the region can accept that certification. No need to start from scratch. That saves precious time and money, and it stops smaller countries from falling through the cracks.

By cooperating this way, ECOWAS states with fewer resources can still keep up with regulatory standards. They benefit from the stronger oversight available in more developed countries, which helps keep everyone on the same page. In the end, mutual recognition isn't just about efficiency. It's a practical way to ensure that even the smaller states have a real say in how AI is governed, especially in crucial sectors like energy.

Avoidance of regulatory arbitrage

When countries don't recognize each other's regulations, you get regulatory arbitrage AI vendors chasing certification in places with weaker rules just to save money or dodge tougher requirements. That's not just a paperwork problem. In areas like energy, it can get dangerous fast. Subpar AI systems slip through, threatening the stability of national power grids or exposing sensitive data. Imagine a vendor certifying an AI system in a country with lax standards, then rolling it out across an entire region. That move undercuts consumer protection everywhere especially in countries trying to keep their standards high. The energy grid's security? Compromised. A harmonized regulatory framework with mutual recognition changes the game. It forces everyone to meet the same strict standards, shutting down the loopholes vendors love to exploit. This isn't just about red tape; it's about making sure only reliable, compliant AI ends up in critical sectors like energy. With mutual recognition in place, you get stronger consumer and government protection, a fairer market, and a whole lot more trust across the region. Safety becomes the baseline, not an afterthought.

Institutional architecture

Mutual recognition should be administered by:

- the ECOWAS AI and Energy Safety Coordination Committee,
- composed of national regulators and technical experts,
- empowered to verify and, where necessary, suspend certifications. These are merely recommendation.

Appeals could be directed to an ECOWAS Administrative Tribunal or the ECOWAS Court for issues implicating rights violations.

Comparative Foundation

The EU's New Legislative Framework (NLF) for product safety provides a strong analogy: conformity assessments conducted in one member state apply EU-wide. This model was upheld judicially in cases interpreting the free movement of goods and services.

Capacity Building and Technical Competence: From Aspirational Literacy to Operational Oversight Capability

This section correctly identifies capacity building as the cornerstone of effective AI governance in West Africa's renewable-energy sector. Comparative evidence from data protection, financial regulation, and energy governance confirms that even well-designed legal frameworks fail where regulators, courts, and institutions lack the technical competence to interpret, audit, and challenge machine-learning systems in practice [6,26].

However, capacity building cannot remain an aspirational objective. For AI governance to function as a substantive safeguard rather than a symbolic commitment, minimum competence thresholds, role-specific skills, and phased capacity targets must be articulated.

Distinguishing AI literacy from machine-learning oversight competence

A critical distinction must be drawn between general AI literacyand specialized machine-learning oversight competence.

- General AI literacy refers to baseline understanding of AI concepts, societal risks, and regulatory principles. This level is appropriate for legislators, senior administrators, and judicial actors who engage with AI governance at a normative or adjudicatory level.
- Machine-learning oversight competence, by contrast, refers to the technical skills required to audit, interpret, validate, and monitor deployed models. This level of competence is essential for regulators, inspectors, and technical reviewers responsible for operational oversight.

This distinction is widely recognized in AI governance literature, which cautions against conflating awareness-raising with effective regulatory capacity [7,24].

Minimum competence requirements for effective oversight

To move beyond abstraction, this paper proposes minimum competence requirements for key institutional actors.

Energy regulators and AI oversight units

Regulatory officials responsible for reviewing or approving AI systems should possess, at minimum, the ability to:

https://doi.org/10.61577/jaiar.2025.100008

- Interpret model documentation (e.g., model cards, validation reports)
- Assess performance metrics relevant to energy systems (e.g., forecasting error rates, optimization objectives)
- Understand dataset provenance, representativeness, and limitations
- Identify risks related to overfitting, data drift, and retraining cycles
- Evaluate whether post-deployment changes trigger renewed compliance obligations

These competencies do not require regulators to design models, but they do require functional literacy in machine-learning validation practices [19,25].

Judicial actors

Judicial competence should focus on:

- Understanding the limits of algorithmic decision-making
- Evaluating expert evidence on model behaviour and performance
- Assessing procedural fairness, explainability, and accountability claims

Judicial education should therefore prioritize interpretive competence, not technical replication, consistent with comparative studies on judicial engagement with complex technologies [29].

Technical infrastructure as an enabler of competence

Human capacity must be supported by a minimum technical infrastructure, without which oversight remains nominal. At a baseline, regulators should have access to:

- Secure data environments for reviewing model outputs and logs
- Tools for basic statistical analysis and performance monitoring
- Version-control and documentation systems to track model updates

OECD studies on regulatory effectiveness consistently demonstrate that institutional competence is inseparable from infrastructural capability [26].

Phase-based capacity development with measurable outcomes

To ensure policy realism, capacity building should be pursued through phased implementation with measurable indicators, rather than open-ended commitments.

Phase I: Foundational literacy (0–2 years)

Target group: Legislators, senior regulators, judges
Outcomes:

- Standardised AI literacy training completed
- Adoption of shared terminology and risk concepts
- Identification of AI focal points within energy regulators

Indicators:

- Percentage of relevant officials trained
- Publication of AI governance guidance notes

Phase II: Operational Oversight Capacity (3–5 years)

Target group: Regulatory inspectors, technical units
Outcomes:

- Ability to review validation reports and datasets
- Routine use of performance benchmarks and drift indicators
- Integration of AI checks into existing compliance workflows

Indicators:

- Number of AI systems reviewed using technical criteria
- Existence of documented audit procedures

Phase III: Advanced and Regional Competence (5+ years)

Target group: Specialist units and regional bodies
Outcomes:

- In-house capacity for independent audits
- Contribution to regional standards and shared registries
- Reduced reliance on external consultants

Indicators:

- Frequency of independent audits
- Participation in ECOWAS-level technical coordination

Phase-based capacity building reflects best practices in regulatory development and avoids the institutional fragility associated with premature expectations of technical mastery [28].

Capacity building as a safeguard against regulatory formalism

By specifying competence thresholds and measurable goals, this section reframes capacity building as a core regulatory safeguard, not a peripheral policy aspiration. Without such specificity, AI governance risks devolving into procedural compliance devoid of substantive oversight, a concern repeatedly identified in both regulatory theory and AI governance scholarship [23,24].

National technical infrastructure investments

AI governance depends on infrastructure. The region requires:

National and Regional Data Centres: To host smart-grid datasets securely and locally, supporting data-sovereignty goals.

Cybersecure Cloud Platforms: Essential for real-time grid analysis and automated control systems.

Smart Metering Infrastructure: With encrypted communication channels to prevent data interception.

High-Bandwidth Fibre Connectivity: Necessary for distributed energy resource management and AI-enabled forecasting.

Regulatory Sandboxes : Allowing experimentation with AI in controlled environments before deployment.

https://doi.org/10.61577/jaiar.2025.100008

Without these investments, regulation becomes symbolic, not operational.

Legal, Human Rights and Social Protection Mechanisms: Integrating a Socio-Technical Rights Framework

This paper correctly situates AI governance within constitutional, human rights, and administrative-law frameworks, particularly with respect to equality, privacy, procedural justice, and socio-economic rights. These legal guarantees are indispensable in the renewable-energy sector, where algorithmic decision-making increasingly mediates access to essential services. However, rights protection cannot be fully realized through legal norms alone. As socio-technical scholarship emphasizes, algorithmic harms emerge from the interaction between legal rules, technical design choices, institutional practices, and social conditions [24,30,31].

Accordingly, this section reframes legal and human-rights protections as embedded socio-technical safeguards, rather than as purely doctrinal constraints.

Equality and non-discrimination as socio-technical obligations

While constitutional equality and non-discrimination norms provide the legal basis for challenging biased algorithmic outcomes, discrimination in machine-learning systems often arises from data selection, feature engineering, and deployment contexts, rather than explicit intent [20].

In the renewable-energy sector, risks include:

- Urban-biased datasets disadvantaging rural or off-grid communities
- Proxy variables (e.g., consumption patterns) indirectly encoding socio-economic status
- Optimization objectives prioritizing efficiency over equitable access

Effective rights protection therefore requires technical equality safeguards, including:

- Dataset representativeness assessments
- Bias testing across socio-economic and geographic groups
- Documentation of trade-offs between efficiency and equity

Embedding these practices within regulatory and constitutional review processes operationalizes equality as a socio-technical requirement, not merely a legal prohibition.

Privacy and data protection beyond formal compliance

The paper 's engagement with privacy and data protection correctly emphasizes consent, purpose limitation, and proportionality. However, privacy risks in machine-learning systems are frequently emergent and systemic, arising from data aggregation, inference, and model reuse rather than from isolated legal violations.

In energy governance, machine-learning systems may infer:

- Household behaviour and occupancy patterns
- Economic vulnerability or energy poverty
- Predictive risk profiles affecting service provision

A socio-technical approach to privacy therefore requires:

- Evaluation of inferential and secondary-use risks
- Limits on model repurposing across regulatory functions
- Technical safeguards such as data minimization, aggregation, and access controls

These measures complement legal privacy guarantees by addressing how privacy harms materialize in practice.

Administrative justice and contestability in algorithmic systems

Administrative-justice principles reason-giving, fairness, and reviewability remain central to AI governance. Yet socio-technical research shows that formal appeal rights are ineffective where affected individuals cannot understand, access, or contest algorithmic decisions [14].

To ensure meaningful contestability, legal protections should be supported by:

- Accessible explanations tailored to affected communities
- Intermediary support mechanisms (e.g., ombudspersons, civil society organizations)
- Procedural accommodations recognizing digital and literacy divides

These measures ensure that administrative justice operates not only in law but also in lived experience.

Socio-economic rights and algorithmic distribution of energy services

The paper's linkage between AI governance and socio-economic rights, particularly access to electricity, is one of its strongest contributions. Socio-technical analysis further underscores that algorithmic systems often reconfigure welfare and service distribution, embedding policy choices within technical artefacts [30,32].

In the renewable-energy sector, machine-learning systems may influence:

- Grid expansion priorities
- Subsidy eligibility
- Load-shedding and rationing decisions

Rights-based protection, therefore requires:

- Transparency around optimization objectives
- Human oversight over value-laden trade-offs
- Social-impact assessments alongside technical validation

These safeguards recognize that technical efficiency decisions are inseparable from normative judgments about social welfare.

Social Protection Mechanisms and Collective Risk Mitigation

Finally, rights protection must extend beyond individual remedies to collective and systemic safeguards. Algorithmic harms often affect communities rather than isolated individuals, particularly in energy infrastructure contexts [34].

Accordingly, this paper supports:

- Collective complaints and representative actions
- Periodic social-impact reviews of high-risk AI systems

https://doi.org/10.61577/jaiar.2025.100008

- Engagement with affected communities during system design and deployment

Such mechanisms align human-rights law with socio-technical realities by recognizing that algorithmic governance redistributes power, risk, and vulnerability.

Ethical, Human Rights, And Social Protection Mechanisms

AI's arrival in the energy sector cuts right to the heart of constitutional rights in every ECOWAS country. We're talking about equality, privacy, dignity, and basic socio-economic rights like reliable electricity access.

Embedding constitutional rights into AI legislation

Legislatures must explicitly integrate rights protections into AI statutes. This includes:

- **Right to equality**
  AI-driven discrimination, whether from biased training data or flawed optimization criteria, can violate constitutional equality clauses.The reasoning in *Enderby v Frenchay Health Authority and Walker* demonstrates that statistical disparities can ground prima facie discrimination claims.
- **Right to privacy**
  Smart-meter data reveals intimate behavioural patterns, triggering privacy protections similar to those articulated in *Klass v Germany*.
- **Right to administrative justice**
  Automated decisions must be explainable and contestable, consistent with *Doody v Secretary of State for the Home Department*
- **Right to socio-economic benefits**
  Electricity access is increasingly recognized as foundational to dignity, health, and development, echoing principles in *Government of the Republic of South Africa v Grootboom*.

Cyber Security for AI-Based Energy Systems: From Technology-Neutral Protection to AI-Specific Threat Governance

The paper correctly recognizes cybersecurity as a central pillar of AI governance in the renewable-energy sector rather than a peripheral technical concern. In energy systems, cyber incidents can generate cascading physical, economic, and human-rights harms, particularly where machine-learning systems influence grid stability, pricing, or access to essential services.

However, traditional cyber security frameworks focused on network integrity, access control, and system availability are insufficiently granular for AI-based energy systems. Machine-learning models introduce distinct vulnerabilities that arise not from software infrastructure alone, but from data dependencies, statistical inference, and adaptive learning processes[34]. Effective governance, therefore requires AI-specific cybersecurity standards, rather than uniform application of generic digital-security controls.

AI-specific cyber threats in renewable-energy systems

Machine-learning systems deployed in energy forecasting, optimization, and grid control are vulnerable to a range of attacks that directly exploit their learning dynamics.

Data poisoning attacks

data poisoning involves the intentional manipulation of training or retraining data to distort model behaviour. in energy systems, this may occur through compromised sensors, falsified grid data, or manipulated weather inputs [35].

Governance implications:

- skewed demand forecasts affecting grid stability
- biased optimization outcomes disadvantaging specific regions
- systemic risk amplified by automated retraining pipelines

Adversarial Attacks on Model Inputs

Adversarial attacks involve subtle perturbations to input data that cause models to produce incorrect outputs while appearing normal to human operators [36].

In AI-driven energy systems, adversarial inputs could:

- Trigger incorrect load-balancing decisions
- Misclassify system states in smart grids
- Induce unsafe control actions in real-time systems

These risks are particularly acute where AI systems operate with limited human oversight.

Model Inversion and Membership Inference Attacks

Model inversion and membership inference attacks allow adversaries to extract sensitive information about training data from deployed models [37].

In energy governance, such attacks may expose:

- Household consumption patterns
- Commercially sensitive infrastructure data
- Vulnerabilities in national or regional grids

These risks intersect directly with privacy, national security, and economic resilience concerns.

Model Theft and Manipulation

Attackers may seek to replicate or manipulate models through repeated querying or insider compromise, undermining both intellectual property and system integrity [38].

Translating AI-specific risks into governance requirements

To avoid treating AI-based energy systems as ordinary digital infrastructure, cybersecurity governance must map specific attack vectors to concrete safeguards.

Data governance and integrity controls

Regulators should require:

- Secure provenance tracking for training and retraining datasets
- Validation and anomaly detection for sensor and operational data
- Restrictions on automated retraining without integrity verification

https://doi.org/10.61577/jaiar.2025.100008

These measures directly address data poisoning risks and align with established ML security research [34].

Robustness and adversarial resilience

For high-risk systems, compliance frameworks should require evidence of:

- Robustness testing against adversarial perturbations
- Stress-testing under abnormal input conditions
- Documentation of known model vulnerabilities

While adversarial robustness remains an open research problem, governance can require demonstrated awareness and mitigation, rather than perfection [36].

Model access and query controls

To reduce model inversion and extraction risks, AI governance standards should mandate:

- Query-rate limiting
- Output minimization (avoiding excessive confidence disclosures)
- Segmentation of sensitive operational models

Such controls are already recognized as effective defensive measures in ML security literature [38].

Incident response and recovery for AI systems

Cyber security obligations should extend beyond prevention to include:

- AI-specific incident reporting obligations
- Rollback mechanisms for compromised or poisoned models
- Post-incident model audits and retraining validation

These requirements reflect the reality that AI systems may require technical recovery, not merely system restoration.

Cybersecurity as a socio-technical governance function

Cybersecurity for AI-based energy systems is not solely a technical issue. It implicates institutional coordination, human oversight, and regulatory competence. Effective protection requires collaboration between:

- Energy regulators
- Cyber security agencies
- Data protection authorities

Given the limited enforcement capacity in many West African states, the paper supports risk-tiered cybersecurity obligations, with the most demanding AI-specific safeguards reserved for systems with high autonomy or systemic impact.

Implications for West Africa's renewable-energy sector

By explicitly addressing AI-specific cyber risks, this section reframes cybersecurity as a core governance mechanism for algorithmic energy systems, rather than a background technical requirement. This approach reduces the risk that AI governance frameworks are applied uniformly across digital infrastructure without recognizing the distinct vulnerabilities introduced by machine learning.

Procurement and Digital Sovereignty: Balancing Transparency, Feasibility, and Enforceable Obligations

This paper correctly identifies public procurement as a critical yet often under-examined lever of AI governance in the renewable-energy sector. Procurement decisions shape not only cost and efficiency outcomes but also long-term dependency structures, accountability pathways, and digital sovereignty. In contexts where machine-learning systems are sourced from global vendors and embedded deeply into energy infrastructure, procurement opaqueness and vendor lock-in pose governance risks that cannot be remedied ex post through regulation alone [39,40].

However, effective procurement reform requires a clear distinction between aspirational policy objectives and legally enforceable procurement requirements, particularly given intellectual-property constraints, market concentration, and capacity limitations within West African states.

Distinguishing policy aspirations from enforceable procurement obligations

To avoid overstatement, this section distinguishes between:

- Aspirational objectives, which guide long-term digital sovereignty and capacity development
- Enforceable procurement requirements, which can realistically be imposed within existing legal and market frameworks

This distinction reflects established procurement-governance practice, which cautions against mandating obligations that public authorities lack the capacity or leverage to enforce [40].

Enforceable procurement requirements: What can realistically be mandated

Certain procurement obligations are both legally defensible and practically enforceable, even in resource-constrained environments:

Transparency and disclosure requirements

Public contracts for AI-based energy systems should mandate:

- Disclosure of system purpose, functionality, and deployment context
- Documentation of model limitations and known risks
- Clear allocation of responsibility between vendor and public authority

These requirements do not require access to proprietary source code and are increasingly recognized as minimum standards in algorithmic procurement [39].

Interoperability and exit provisions

To mitigate vendor lock-in, procurement contracts should include:

- Data portability obligations
- Use of open standards where feasible
- Contractual exit clauses enabling system migration or replacement

Such provisions are widely used in digital-infrastructure procurement and are compatible with competitive markets [40].

https://doi.org/10.61577/jaiar.2025.100008

Audit and access rights

Rather than mandating full source-code disclosure, contracts can require:

- Third-party audit rights
- Access to model documentation and performance logs
- Cooperation in regulatory inspections

This approach balances intellectual-property protection with public-interest oversight [6].

Aspirational objectives: Guiding long-term digital sovereignty

Other goals, while normatively compelling, are better framed as aspirational policy directions rather than immediate procurement mandates.

Source code access

Mandatory source-code access for all AI systems is often neither feasible nor legally sustainable, particularly in competitive global markets. Instead, policy frameworks should:

- Encourage open-source or open-architecture solutions where strategically appropriate
- Promote negotiated access arrangements for high-risk or mission-critical systems
- Support domestic research and development ecosystems over time

This calibrated approach avoids discouraging vendor participation while advancing transparency incrementally.

Technology transfer and localization

Technology transfer requirements must account for :

- The absorptive capacity of local institutions
- The risk of symbolic compliance without substantive skill transfer
- Long time horizons required for meaningful capacity development

Comparative evidence suggests that training obligations, joint development projects, and local maintenance requirements are more effective than formal technology-transfer clauses alone.

Procurement as a capacity-building instrument

Procurement should be used not only to acquire technology but also to build institutional and technical competence, consistent with Section 9.4. Realistic measures include:

- Requiring vendor-led training for regulators and operators
- Mandating knowledge-sharing during system deployment
- Including maintenance and documentation obligations that support long-term autonomy

Such measures strengthen digital sovereignty without imposing unenforceable demands.

Avoiding symbolic sovereignty claims

Finally, the paper cautions against symbolic assertions of digital sovereignty unsupported by institutional capacity or contractual leverage. Digital sovereignty is better understood as a graduated condition, achieved through cumulative procurement choices, contractual safeguards, and domestic capacity development, rather than through categorical mandates.

Avoiding dependency on foreign AI Systems

Without deliberate policy intervention, West Africa may fall into digital dependency, where foreign firms control critical energy algorithms. To prevent this:

- enforce data localization rules;
- require technology-transfer provisions in contracts;
- ensure algorithmic sovereignty through source-code escrow arrangements;
- promote regional AI manufacturing and development supply chains;
- limit exclusive, long-term vendor lock-in contracts.

This approach mirrors broader concerns raised by scholars about “digital colonialism” in African digital ecosystems [41].

Encouraging local innovation

Technological sovereignty requires local innovation ecosystems.

Governments should:

- fund national AI-energy research centres;
- establish AI fellowship programmes;
- support university labs;
- incentivise startups developing load-forecasting, anomaly-detection, and demand-response tools;
- create national and regional AI competitions.

This approach aligns with Agenda 2063’s emphasis on African innovation and industrial development.

Conclusions

This paper lays out a detailed roadmap for how West Africa can govern AI in its renewable energy sector. It digs into everything from changing laws and building new institutions to making sure countries across the region work together. There’s focus on training, protecting human rights, cybersecurity, and how governments buy technology. The approach borrows what works from the EU AI Act but stays rooted in African legal traditions and priorities. The goal is clear: West Africa needs a system that fits the region, respects rights, encourages innovation, improves energy access, and keeps the region stable.

Acknowledgement

The use of AI was used in carrying out several findings in this paper. It was further employed in rephrasing certain keywords for a better understanding.

Disclosure Statement

No potential conflict of interest was reported by the author

https://doi.org/10.61577/jaiar.2025.100008

References

1. Craig P. Administrative law (7th ed.). Sweet & Maxwell. 2012. Available at: https://books.google.co.in/books/about/Administrative_Law.html?id=ZL4bYAAACAAJ&redir_esc=y
2. Baldwin R, Cave M, Lodge M. Understanding regulation: theory, strategy, and practice. Oxford university press; 2011.
3. Scherer MU. Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. Harv. JL & Tech. 2015;29:353. https://dx.doi.org/10.2139/ssrn.2609777
4. Lodge M, Wegrich K. Managing regulation: Regulatory analysis, politics and policy. Bloomsbury Publishing; 2012. https://doi.org/10.1007/978-1-137-26552-4?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle
5. Moses LB. Artificial intelligence in the courts, legal academia and legal practice. Australian Law Journal. 2017;91(7):561. https://ssrn.com/abstract=3742515
6. Coglianese C, Lehr D. Regulating by robot: Administrative decision making in the machine-learning era. Geo. LJ. 2016;105:1147.
7. Veale M, Borgesius FZ. Demystifying the draft EU artificial intelligence act. arXiv preprint arXiv:2107.03721. 2021. https://doi.org/10.9785/cri-2021-220402
8. OECD. Artificial intelligence in society. 2019. https://www.oecd.org/en/publications/2019/06/artificial-intelligence-in-society_c0054fa1.html
9. Hong T, Fan S. Probabilistic electric load forecasting: A tutorial review. Int J Forecast. 2016;32(3):914-938. https://doi.org/10.1016/j.ijforecast.2015.11.011
10. Voyant C, Notton G, Kalogirou S, Nivet ML, Paoli C, Motte F, Fouilloy A. Machine learning methods for solar radiation forecasting: A review. Renewable energy. 2017;105:569-582. https://doi.org/10.1016/j.renene.2016.12.095
11. Widmer G, Kubat M. Learning in the presence of concept drift and hidden contexts. Machine learning. 1996;23(1):69-101. https://doi.org/10.1023/A:1018046501280
12. Gama J, Žliobaitė I, Bifet A, Pechenizkiy M, Bouchachia A. A survey on concept drift adaptation. ACM computing surveys (CSUR). 2014;46(4):1-37. https://doi.org/10.1145/2523813
13. Conejo AJ, Carrión M, Morales JM. Decision making under uncertainty in electricity markets. New York: Springer; 2010. https://doi.org/10.1007/978-1-4419-7421-1
14. Citron, D. K., & Pasquale, F. The scored society. Washington Law Review. 2014(89):1–33. https://ssrn.com/abstract=2376209
15. Karnouskos S. Artificial intelligence in digitalized energy systems. IEEE Industrial Electronics Magazine. 2020;14(4):55–68.
16. Fuller LL. The morality of law. Yale University Press. 1969. https://doi.org/10.2307/2217903
17. Ai H. High-level expert group on artificial intelligence. Ethics guidelines for trustworthy AI. 2019. Available at: https://www.aepd.es/sites/default/files/2019-09/ai-definition.pdf
18. European Commission. Proposal for a regulation laying down harmonised rules on artificial intelligence (AI Act). 2021. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence
19. Doshi-Velez F, Kim B. Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608. 2017. https://doi.org/10.48550/arXiv.1702.08608
20. Barocas S, Selbst AD. Big data's disparate impact. Calif. L. Rev.. 2016;104:671. http://dx.doi.org/10.15779/Z38BG31
21. Black J. Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regulation & governance. 2008;2(2):137-164.
22. Gebru T, Morgenstern J, Vecchione B, Vaughan JW, Wallach H, Iii HD et al. Datasheets for datasets. Communications of the ACM. 2021;64(12):86-92. https://dx.doi.org/10.1145/3458723
23. Power M. The audit society. Oxford University Press.1997. Available at: https://global.oup.com/academic/product/the-audit-society-9780198296034?cc=in&lang=en&
24. Selbst AD, Boyd D, Friedler SA, Venkatasubramanian S, Vertesi J. Fairness and abstraction in sociotechnical systems. InProceedings of the conference on fairness, accountability, and transparency. 2019;59-68. https://doi.org/10.1145/3287560.3287598
25. Mitchell M, Wu S, Zaldivar A, Barnes P, Vasserman L, Hutchinson B, et al. Model cards for model reporting. InProceedings of the conference on fairness, accountability, and transparency. 2019:220-229. https://doi.org/10.1145/3287560.3287596
26. OECD. The governance of regulators. 2014.
27. Mahoney J, Thelen K, editors. Explaining institutional change: Ambiguity, agency, and power. Cambridge University Press. 2009.
28. OECD. International regulatory co-operation: Addressing global challenges. 2013
29. Susskind R. Online courts and the future of justice. Oxford University Press; 2019. https://doi.org/10.1093/oso/9780198838364.001.0001
30. Winner L. Do artifacts have politics? Daedalus. 1980;109(1):121-136. http://www.jstor.org/stable/20024652?origin=JSTOR-pdf
31. Jasanoff S. States of knowledge: The co-production of science and social order. Routledge. 2004. https://doi.org/10.4324/9780203413845
32. Yeung K. Algorithmic regulation: A critical interrogation. Regulation & governance. 2018;12(4):505-523. https://doi.org/10.1111/rego.12158
33. Eubanks V. Automating inequality. St. Martin's Press. 2018. https://doi.org/10.24377/LJMU.prism.vol2iss1article296
34. Biggio B, & Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition. 2018;84:317-331. https://doi.org/10.1016/j.patcog.2018.07.023
35. Biggio B, Nelson B, Laskov P. Poisoning attacks against support vector machines. arXiv preprint arXiv:1206.6389. 2012. https://doi.org/10.48550/arXiv.1206.6389
36. Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. 2014. https://doi.org/10.48550/arXiv.1412.6572
37. Fredrikson M, Jha S, Ristenpart T. Model inversion attacks that exploit confidence information and basic countermeasures. InProceedings of the 22nd ACM SIGSAC conference on computer and communications security. 2015:1322-1333. https://doi.org/10.1145/2810103.2813677

https://doi.org/10.61577/jaiar.2025.100008

38. Tramèr F, Zhang F, Juels A, Reiter MK, Ristenpart T. Stealing machine learning models via prediction {APIs}. In25th USENIX security symposium (USENIX Security 16). 2016:601-618. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer

39. Kitchin R. Big Data, new epistemologies and paradigm shifts. Big data & society. 2014;1(1):2053951714528481. https://doi.org/10.1177/2053951714528481

40. OECD. Public procurement in the digital age. 2020.

41. Nyabola N. Travelling While Black: Essays Inspired by a Life on the Move. Oxford University Press; 2021.

https://doi.org/10.61577/jaiar.2025.100008