

<https://doi.org/10.59298/NIJCIAM/2025/71.1019>

Algorithmic Governance and Public Accountability: Audits, Transparency, and Harm

Tarcisius Niwagaba

Humanities Education Kampala International University Uganda

Email: tarcisius.niwagaba@kiu.ac.ug

ABSTRACT

Algorithmic systems are increasingly embedded in public administration, shaping decisions in areas such as social services, law enforcement, urban governance, and financial regulation. While these systems promise efficiency, scalability, and data-driven insights, their deployment also raises significant concerns regarding transparency, fairness, discrimination, and accountability. This paper examines the governance of algorithmic systems through three central mechanisms: audits, transparency, and harm assessment. It explores how algorithmic governance frameworks can ensure the responsible deployment of artificial intelligence (AI) systems while safeguarding public trust and democratic values. The study reviews mechanisms of internal and external audits, emphasizing the importance of standardized auditing procedures, performance metrics, and independent oversight to evaluate algorithmic performance and detect biases or unintended consequences. It further analyzes transparency practices, including data provenance, model disclosure, explainability, and governance records, which enable citizens, regulators, and stakeholders to understand and scrutinize automated decision-making processes. In addition, the paper discusses various forms of harm arising from algorithmic systems, ranging from individual-level discrimination and privacy violations to systemic risks that undermine democratic institutions and social cohesion. Drawing on international case studies from municipal governments and public service delivery contexts, the paper highlights both the opportunities and limitations of current governance approaches. It concludes that effective algorithmic governance requires multi-layered accountability structures involving policymakers, public institutions, industry actors, and civil society. Strengthening auditing standards, enhancing transparency, and establishing robust mechanisms for harm mitigation and redress are essential to ensure that algorithmic systems operate in ways that promote fairness, protect human rights, and uphold democratic accountability.

Keywords: Algorithmic Governance, Public Accountability, Algorithmic Audits, Transparency and Explainability, and Algorithmic Harm.

INTRODUCTION

Algorithmic systems increasingly influence decisions and services in public administration. Technological advances and the rising ubiquity of public datasets intensify interest in these systems, with complex Artificial Intelligence (AI) solutions gaining traction for generating valuable insights hidden in massive datasets [1]. Despite their transformative potential and the zero marginal cost for their sharing and deployment, algorithmic systems may yield considerable risks, including unintended algorithmic consequences, discrimination and unequal treatment, opacity, alienation, and communication degradation [2]. Algorithmic governance is necessary to

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

address these risks, relying on audits, transparency, and public accountability to build citizen trust in automated solutions, ensure equitable service access and quality, mitigate physical and psychological harm, foster innovation, and promote robust AI adoption [1, 2]. Audits permit informed estimation of algorithmic systems' inherent risks and their management. Although audits based on established, standardised approaches develop gradually, algorithmic systems already undergo considerable scrutiny for public services. The governance of algorithmic systems in public administration should therefore be investigated now [3]. Independently audited, publicly documented evidence on processes and outcomes associated with automated decision-making supports robust governance. Transparent protocols and records for algorithmic decision-making enable wider scrutiny and participatory assignment of fundamental societal values (garanties fondamentales) as society retains agency over every large-scale socio-technical solution. Information about datasets and models underpinning algorithmic solutions increases awareness of potential opportunities and limitations [4].

Conceptual foundations of algorithmic governance

Algorithmic governance occupies a central position in efforts to address public concern about the impacts of algorithmic systems on society [3]. As algorithmic systems permeate both private and public sectors, the use of machine learning, artificial intelligence (AI), and related technologies raises questions about fairness, equity, discrimination, human rights, social values, control, and unintended consequences [4]. The term 'algorithmic governance' designates the different strategies that might be employed to address these concerns through intervening with the design, operation, and broader socio-technical context of algorithmic systems, especially in the public sector context where the instruments of oversight and control are often, though not exclusively, enshrined in law [5]. Audits, transparency, and definitions of societal harm are pivotal dimensions of algorithmic governance, and these present grounds for a review of what is known about these concepts and the available options for their implementation [6].

Mechanisms of Audits in Algorithmic Systems

Audits, transparency, and harm are three central mechanisms of algorithmic governance. To mitigate the potential for harm, algorithmic systems must undergo audits [5]. Various configurations exist for implementing algorithmic audit mechanisms [4]. Internal or self-governance can involve validation through examination by the deploying organization, while external and independent audits may include scrutiny by hired third parties or public interest groups. The need for performance metrics in both self-governance and third-party audits calls for established auditing procedures that hold algorithms accountable with specified criteria [1]. Various contexts in which individuals or groups experience disadvantageous treatment aggregate to broader societal harms that can exceed the sum of individual effects [3]. Algorithmic audits provide a means to try to investigate the proper functioning and consequences of sociotechnical systems [2]. The term encompasses a looser set of methods, ranging from formal verification of particular performance characteristics to participatory evaluations that assess overall perceived ethical compatibility. The audit concept, therefore, spans technical procedures that require considerable technical expertise and legal rights to access and analyze relevant datasets, as well as participatory evaluations that may be carried out by numerous social actors without any specific analytic training [6].

Internal Audits and Validation

Algorithmic governance relies on public accountability to facilitate scrutiny, provide the basis for protection against risks, and enable redress against harm [5]. To advance this accountability framework, audits that improve algorithmic performance, foster transparency about algorithm use and system operation, and measure the extent and severity of harm should be prioritized [1, 5]. Internal audits and validation are applicable to both algorithmic and non-algorithmic systems. They assess adherence to established standards and provide a foundation for the transparency required to judge accountability. Implementation of audit mechanisms permits active learning and knowledge-sharing across similar implementations in diverse contexts and domains [7]. Audits are essential in governance frameworks, as algorithms and data underpin critical societal functions. Nevertheless, the governance of publicly funded algorithms remains largely unexplored in research or practice. Regulatory and legislative solutions are emerging, but practical implementation across differing contexts requires a deeper understanding [8].

External and Independent Audits

External-facing audits, such as Facebook's, frequently take place prematurely, exposing processes to external scrutiny before internal assessments have identified and addressed weaknesses. Strengthening internal audit mechanisms remains essential prior to engaging with external challenges [4]. Involvement of external experts for targeted, multi-year internal audits contributes to process enhancement and connects AI accountability with existing risk management frameworks, allowing for the prioritization of AI-related risks alongside other corporate uncertainties [5]. The development of standardized AI audit services is ongoing; initiatives like IEEE's Ethics

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Certification Program for Autonomous and Intelligent Systems strive to improve transparency and accountability, although these standards are still evolving [6]. The European Commission is progressing toward delegated acts to implement independent compliance audits as part of a risk management cycle that includes risk assessments. Uncertainties persist regarding the identity of independent auditors and whether they will evaluate the quality of internal risk assessments [7]. Recommendations for independent audits include assessment of the quality and methods of internal risk evaluations, incorporation of experts on systemic risks and algorithms, and, ideally, independent risk assessments employing a risk scenario audit approach. Very Large Online Platforms (VLOPs) are obliged to report internal risk-assessment results to authorities and make them publicly accessible. To ensure transparency and accountability, VLOPs should also provide a comprehensive methodological description of their assessments, detailing hypotheses and metrics employed, and disclose audit processes and tested scenarios [6].

Performance Metrics and Auditing Standards

Performance metrics and standards for auditing are vital for diagnosing problems and ensuring accountability in algorithmic decision-making. Clarity and transparency of algorithmic features enable stakeholders to contest decisions and seek redress [6]. Lack of interpretability hampers the detection of underperforming models, leading to overreliance and limited human oversight [8]. Public administrators must demand tools compatible with their roles, properly vetted, and continuously monitored, and receive training to understand these tools. Developers and system architects should evaluate models for fairness, bias, and transparency to guarantee comprehensibility and diagnosability [6]. Difficulties in contesting algorithmic decisions exemplified by the COMPAS risk assessment in US courts underscore the necessity for standards and auditing processes. Without insight into assessment criteria, individuals cannot meaningfully challenge wrongful actions or pursue redress, highlighting the importance of auditing and performance evaluation [1].

Transparency as a Governance Principle

Informed citizens need access to information that government actors do not make available proactively. Transparency is becoming a widely adopted governance principle [6]. Data provenance provides information about data sources, their preparation, and their transformation into derived datasets. Model disclosure involves public release of a model's architecture and parameters [3]. Providers of machine-learning-based public services, such as recommendation systems, have started to publish the model architecture and hyperparameters used by their systems to enable others to inspect the information [5]. Explainability and interpretability techniques support existing model architectures without requiring a provider to furnish an explicit specification of a model, while sought for other reasons, can also contribute to algorithmic governance [6]. Open protocols establish common structures that can facilitate interoperability, enabling information exchanges and collaborative arrangements among different agents. Governance records document decision-makers and procedures, specifying how policies are established, amended, and enacted, and can help citizens comprehend decision-making processes [7, 8].

Data Provenance and Model Disclosure

Algorithmic systems often rely on multilayered models built on massive datasets; it is both impractical and undesirable to openly publish the complete training materials [6]. Nevertheless, insight into the provenance of data and models at different abstraction levels aids in understanding the nature and limitations of system design 9. Traces of how data items were generated, transformed, or selected can provide a contextual view of the corresponding inputs and outputs of a deployed algorithm, indicating potential biases or issues [4]. Likewise, a description of the classes of models, modeling strategies, architectural choices, and tuning processes clarifies capabilities or the kinds of tasks for which the system was intended [8]. A lack of transparency is characteristic of algorithmic systems, as continual involvement of information obscures how inputs are related to outputs [5]. Internally generated metadata, often stored with the model or data, can illuminate aspects of the design process that are relevant to external stakeholders. While information cannot be restricted to a specific subsystem, clear explanations of the system's use and context, delineating the algorithm's responsibilities vis-à-vis other components, support informed judgment regarding risk and appropriateness [5]. Transparency of data provenance, model construction, and the ongoing evolution of the algorithm, including changes made and unchanged assumptions, also helps calibrate expectations of the system and fosters better governance through broader understanding [3].

Explainability and Interpretability

It has been noted that “an AI system is accountable to the degree that a third party can understand the system, can decipher its behavior, and can articulate how the system's output is causally linked to its input” [1]. Accountable systems allow understanding of a system's use and facilitate internal and external challenge and oversight 10. Understanding is framed in terms of explainability (conveying how decisions are made) and interpretability

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

(intuitive understanding of how a decision would respond to certain inputs) [8]. System understanding enables owners to interpret results, spot faults, and avoid improper deployment of flawed systems [7]. Algorithmic decision-support systems are characterised by sophisticated, data-driven algorithms; yet algorithmic audits often depend only on a query-response mechanism, leaving understanding of algorithmic operation limited [5]. Though complex algorithms can be audited through advanced diagnostics, this rarely occurs in practice. Algorithmic design and operation must be accessible to public agency employees, whether direct users or intermediaries on behalf of citizens [6].

Open Protocols and Governance Records

Transparency provides the foundation for algorithmic governance. It is a broad concept that encompasses the documentation, discussion, and justification of every decision made during the governance of an algorithmic system, along with periodic assessments of whether the anticipated objectives are being met [1]. Three categories of information are particularly relevant to algorithmic systems [10]. Protocols used to govern the development and use of an algorithmic system; [2]. records of how those protocols have been implemented; and 3. evaluations of whether the protocols and their implementation are achieving the desired results. The first category is described in more detail in the next section [9]. This section focuses on the other two categories. Maintaining a governance record is a hallmark of sound corporate governance; similarly, maintaining a governance record for algorithmic systems is an essential element of algorithmic governance. Records are consultable documentation of how the protocols of governance have been implemented. A governance record should catalogue all the algorithmic systems developed in an organization, the problems they address, and the procedures followed in the life cycle of each system [7]. Such a record is indispensable for enabling effective auditing [5]. Open protocols and comprehensive governance records strengthen accountability and enable redress. A democratic platform provides people with assurances that public resources are being used on their behalf and enables the development and implementation of mechanisms such as transparent protocols and governance records that foster accountability. These mechanisms help answer key questions related to algorithmic systems: What criteria are being used? How are they decided? Who decides? What public interest considerations, if any, underlie the use of the algorithm? How are the interests of affected individuals and relevant third parties taken into consideration? [6, 7]

Public Accountability Frameworks

Algorithmic governance seeks to ensure an organization's algorithmic and data practices are aligned with its mission. While audits are a key component of governance, they can examine only specific aspects, given confidentiality concerns, and regulators are often limited in their powers and scope [12]. This section explores broader frameworks for public accountability that bolster and complement audits. A clear understanding of the relevant legal and regulatory environment shapes the governance framework an organization can adopt. Civic oversight, community participation, and regulatory monitoring formalize options for external review, deliberation, feedback, and dialogue [9]. Enabling the public to understand the potential consequences and risks of specific algorithmic systems facilitates meaningful scrutiny of algorithmic and data practices and reinforces the public accountability critical to governance [8]. The framework of human rights law specifies obligations, responsibilities, and remediation pathways for systematic abuses of algorithmic systems [3]. This framework views governance not just as prevention but also as an effort to mitigate harm and enable redress. Recognizing the dynamism of algorithmic systems, clear pathways for recourse at the earliest indications of harm mitigate risks of escalation and prolongation. Capitalizing on existing, high-profile initiatives aids design and adoption [11].

Legal and Regulatory Considerations

Algorithmic management, widely adopted to improve productivity and efficiency, raises concerns about its impact on workers. Steps can be taken to regulate it, such as legal frameworks that set requirements for audits on algorithmic systems [2]. Purpose and goals should also be clear. One such aim could be to change the design of systems that influence workers. Assessment should not only focus on measurable effects but also pay attention to normative frameworks, values, and multiplicity of harms involved [3]. Balancing out the obligation of reporting without disrupting redrawing expectations and endangering the environmental movements is delicate 2. Conversely, facilitating a plurality of audiences while maintaining meaningful activity is also complex. Thus, consideration of adjacent yet distinctive ethics, such as bioethics, should be encouraged [6].

Civic Oversight and Participatory Mechanisms

The important principle of participatory governance in algorithmic systems acknowledges the essential role of civic oversight and public involvement. Despite algorithms acting on behalf of government entities and serving the public interest, state authorities must not act as sole gatekeepers [2]. Algorithmic systems frequently embody governmental power and authority, yet the technological, legal, and ethical foundations of their operation often elude public understanding [1]. Such dynamics can lead to blind trust, disengagement, and the acceptance of

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

unsatisfactory circumstances. Public engagement can assist in identifying and addressing dangerous societal conditions, articulating needed policy solutions, and fostering a shared understanding of algorithmic applications, benefits, and risks [13]. Participatory mechanisms allow citizens to contribute knowledge, evaluation, and social norms, thereby influencing the design of algorithmic solutions and their delimitation of use. They can also channel information about adverse effects that government organizations may not directly observe [11]. Mass surveillance activities operate covertly, and those targeted may be unaware of their involvement; participatory oversight provides a larger lens for scrutiny [13]. Civic engagement cultivates an understanding of how algorithms function, the problems they aim to solve, their impacts, and the benefits versus disadvantages. Since democratic governments derive authority from the population and rely on procedural legitimacy, public transparency and participation reinforce accountability [12].

Consequences, Redress, and Remediation Pathways

Organizations adopting algorithmic decision-making are often held liable for the negative impacts of those systems and directly accountable for ameliorating identified harm [1]. Analysts highlight that determining the technical causes underlying system behaviour is inherently difficult. A lack of transparency impedes effective contestation and hinders understanding of emergent phenomena. Consequently, intervention opportunities diminish, the learning feedback loop shrinks, and post-facto accountability mechanisms weaken [13]. Roles and responsibilities shift from technological to governance considerations, raising important questions: Which actors are empowered to deliver the necessary knowledge? How can they engage effectively with algorithmic systems? The disproportionately high stakes associated with socio-technical systems increase the urgency for effective, confident, and timely public accountability arrangements [3]. Public authorities and organizations fostering algorithmic decision-making should pursue an expansive framing of consequences, redress, and remediation pathways [14]. Consideration must extend beyond organizational liability for performance failures or the direct causes of violation or harm. Public accountability frameworks accommodate a potentially broad array of contributors, responsibilities, and information needed to fulfil personal accountability obligations [12].

Harm Arising From Algorithmic Systems

Algorithmic decision systems raise public concerns about harm arising from their deployment, endorsement, or continued use [11]. Such harms affect individuals or groups directly, impacting privacy, autonomy, or discrimination; or they remain systemic, impacting the social fabric and societal susceptibility to shocks or disinformation [3]. Algorithmic systems are associated with numerous risks, necessitating methods for rigorous risk assessment and reduction [2]. Without systematically addressing algorithm-related risks, society risks systemic, cascading harm with unprecedented intensity, velocity, and scale, and a decline in overall societal robustness to either algorithmic or non-algorithmic shocks [1]. Robust, auditable methodologies for assessing and, where possible, mitigating these risks must thus be developed as a precondition for deploying algorithmic systems [3].

Harms to Individuals and Groups

Algorithmic systems can inflict considerable harm on individuals and groups, including the deprivation of rights and freedoms, the promotion of discrimination or exclusion, and the manipulation of autonomy or consent [13]. The potential for harm increases in contexts marked by fragility, vulnerability, looser legal frameworks, limited institutional capacity, or weaker regulatory oversight [12]. The consequences of algorithmic governance-related harm, including the erosion of public trust in institutions, social fragmentation, polarization, and the weakening of resilient democracies, may be even more acute when these conditions prevail [12]. The recognition of algorithmic system-related harm as a global problem is growing, particularly in human rights and international development discussions [13]. Human rights law offers a complementary framework to the human-centric and social welfare approaches, focusing on social systems, preventability, objective analysis, and the articulation of dimension and cause [3].

Systemic Risks and Societal Impact

Algorithmic systems may produce various types of harm with significant societal implications. Such impacts may extend to entire populations, affect large numbers of people simultaneously, or pose a significant risk to college or society as a whole [8]. Systemic risks arise when algorithmic governance reduces or removes institutional checks and balances through black-box systems, drives a shift from social to private gain, or otherwise erodes publicly accountable decision-making [2]. The proliferation of algorithmic systems heightens systemic risk, particularly in major technologies such as machine learning, natural language processing, and generative art [13]. These developments further entrench existing currents toward privatization, value extraction, and automated decision-making in urban governance 1. Serious limitations and systemic inequalities in technology, machine learning, and governance throughout the public sphere impede accountability for social and institutional impacts [11].

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

Algorithmic decision-making with feedback loops intensifies drift in accountability norms among affected populations [12].

Risk Assessment and Mitigation Strategies

Algorithmic systems increasingly permeate societal domains, thereby shaping people's lives through decisions concerning education, employment, law enforcement, loan approval, insurance, and other critical areas [3]. These systems pose risks to individuals, groups, and society at large. Auditing and associated transparency measures enable stakeholders to mitigate potential harm through various strategies [1]. Public accountability frameworks assure that such measures are appropriately enforced. Risk mitigation in algorithmic governance encompasses frameworks, protocols, techniques, metrics, and other mechanisms for assessing and responding to harmful effects. Risks are classified according to the type of harm they may generate and whether they affect individuals or disproportionately impact specific groups [4]. The following typology distinguishes these concepts. Individual-level harms include privacy violations via surveillance, algorithmic manipulation leading to misinformation, and cybersecurity attacks causing service disruption, data leaks, or other critical failures. Group-level harms range from discrimination and exclusion arising from biased data, through economic inequality, to threats to freedom, democracy, and civil rights. Systemic risks include deterioration of the public sphere via diminished trust and increased polarization, cybercrime and fraud resulting from inadequate protection of sensitive data, and eroding social cohesion caused by algorithmic discrimination that sustains pre-existing biases and disparities [5]. Societal-level effects encompass a lowering of democratic engagement, challenges to freedom and identity, erosion of government functioning, and conflicts obstructing legitimate social order. A parallel set of mitigation strategies corresponds to these categories. To counter individual-level effects, notification and explainability strategies can inform impacted individuals about algorithmic decisions and systems employed, thus clarifying the appropriateness of such decisions [3]. The expected value of notifications follows from the degree of understanding they afford about actions taken under prevailing policies. The utility of explainability stems from stakeholders' capacity to comprehend the relationship between data inputs and algorithmic outputs. Group-level mitigation strategies include external attestation of system significance and societal-benefit assurance [5]. A declaration on social benefits and intended impacts should accompany each algorithmic deployment, enabling cross-institutional progress evaluation and encouraging collaboration among developers and agencies to enhance system performance and address emerging risks [6]. Systemic concerns can be mitigated via sharing, cooperation, and concerted initiatives. Information about the specific domain addresses and operating principles of deployed systems is pertinent for auditing and must thus accompany risk declarations [7]. Considerable potential exists for redundancy in system implementation across agencies; straightforward enumeration of governmental systems could aid in identifying collaborative opportunities and affording agencies added insight into the systems entrusted to them [13].

Case Studies and Empirical Evidence

Algorithmic systems for public service delivery in an era shaped by the rise of artificial intelligence (AI) have provoked public controversy concerning their deployment, their impact on people's lives, and the justification, risk management, and redress associated with these systems [13]. Increasing calls for algorithmic transparency in public service delivery, notwithstanding the multiple debates regarding data privacy, national security, and commercial confidentiality, suggest that the governance of such systems and algorithmic systems in general constitute important areas of further exploration [10]. The City of Gothenburg, Sweden, has emphasised a strong commitment to transparency by releasing the results of internal audits and conducting an external audit of its case management system, increasing public insight into the audit outcomes. The results exposed serious risks with the city's algorithmic system [11]. In addition to algorithmic transparency, the city also demonstrated the importance of publishing audit results for citizens' understanding of algorithmic systems and of revealing the AI auditing portfolio to guide the further elaboration of algorithmic auditing standards [14]. The City of Zurich, Switzerland, has commenced a series of external audits on automated decision-making systems. The supply partner responsible for the provision of Genève's public transport model has undertaken at least two external audits of its system, raising questions about the audit independence principle and relevant auditing standards. Moreover, despite the existence of cases, it is challenging to construct relevant indicators measuring harm arising from those automated decision-making systems employed in public services [4]. Algorithmic systems warrant priority consideration because of their systematic application in major urban cities, including manufacturing, traffic management, logistics, automatic-writing digital emblem abstractions, and lighting systems, among others. The percentage of system failures and negligence reports concerning algorithmic systems continually surges across the transportation and housing sectors [1]. Moreover, machine learning is currently considered by municipalities to optimise multi-faceted building permits on a large scale. Nevertheless, few municipalities have sought algorithm

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

audits, and an absence of measurements regarding harm has been recorded. In the context of automatic authoring systems for marketing purposes, machine-generated text has perpetuated prejudices and stereotypes concerning particular ethnic groups [5].

Case Study A: Transparency in Public Services

Algorithmic decision-making is increasingly employed in various public services, creating a pressing need for accountability frameworks [6]. In Amsterdam, the use of algorithms within the municipality for tasks such as energy consumption analysis, housing offer selection, and selection for social support has exceeded levels seen in other major cities [7]. Nevertheless, municipal elected officials, including the mayor, acknowledge that algorithmic governance poses a challenge to the principles of democracy. Although data scientists are involved, the current governance structure does not adequately address issues of public oversight [8]. Regulations governing civil service positions have previously hindered the direct involvement of members of parliament in decision-making for such processes, fostering a notion of openness without a clear understanding of what that entails under algorithmic governance. Amsterdam's municipal government recognizes that there are still many unknowns associated with algorithmic governance. As algorithms proliferate, public authorities will increasingly assume responsibility for content and decision logic, yet the kind of public accountability envisaged must be specified [14]. In the province of Drenthe, public organizations face challenges in managing large volumes of information. The municipality of Assen employs algorithmic decision-making within its network security department to advise on security measures and strategies. Consequently, the municipality's public cohort has become deeply intertwined with algorithms, rendering accountability to monitor obligations and arrangements difficult to maintain [15].

Case Study B: Audit Outcomes in Surveillance Contexts

Algorithmic governance aims to mitigate harms arising from algorithmic systems [15]. Governance principles derive from transparency, audit outcomes expose potential and entrenched harms against certain groups, and civic frameworks establish shared responsibility for understanding and addressing identified problems [10]. A study featuring a large audit dataset across a spectrum of algorithmic systems highlights how governmental and civic actors use varied information to engage with different systems and that harmful outcomes experienced jointly by groups exhibit significant overlap despite dissimilar official use cases [4].

Case Study C: Governance of Automated Decision Systems

Automated decision-aiding systems by one large municipality suggest a limited early-adoption phenomenon across the automation continuum amid scrutiny of algorithmic decision-making (ADM) globally [5]. Being conscious of attendant socio-technical issues and mitigating risks promises to mobilise support and keep ADM within jurisdictions [7]. Through specified advisory terms and informal surveys, a scene-setting account traces public administrators' broad concerns about governance and communication of ADM systems across nine municipality departments, adapted from an international framework by [14]. A link to regional public-service values of trust and inclusiveness muting widespread unease about harm motivated prioritising governance and communication channels over substantive guidance. A target decision-aiding use case involved loan eligibility regarding housing, a concern where affected citizens' ability to appeal decisions hinged upon transparency and meaningful access to decisions implicated by an algorithm [15]. Governance checks at the outset mandated human control over decisions and permitted transparency into the function of the loan-eligibility algorithm. A wide-open search for transparency then uncovered two specific signal-extraction themes, risk factors highlighting both loan loss and applicant deprivation, and more general modelling that segregated advice thresholds from current information in previously unrecognised ways [16]. The signal-extraction requirement may constitute an item within a wider literature on algorithmic transparency focused on disclosure type rather than content that recognises algorithm function and supporting governance, played August 2021 [1].

Methodological Considerations for Research and Policy

The audit and assessment of algorithmic systems and related artefacts by independent researchers and civil society organizations remains hampered by institutional secrecy, data access constraints, and information asymmetries [13]. These barriers complicate empirical research efforts and obstruct investigations intended to hold decision-makers and implementers accountable [1]. Algorithmic harms may vary in intensity from trivial to life-altering and high-stakes. Risk assessments, therefore, should be conducted at both granular and macroscopic levels to ascertain both specific consequences on individuals, communities, and entities and broader potential for societal harm. Studies constrained by limited or asymmetric access may yield relevant insights even when lacking full information regarding the precise nature of public and proprietary data involved [10]. Overly prescriptive and normative definitions of specific algorithm-generated harms may deter investigation into additional publicly unknown artefacts exhibiting significant risk at present [9]. Referential analyses, typologies, and categorization

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

systems helped articulate principles, indicators, mathematical vocabularies, and qualitative frameworks that govern algorithmic public-sector policy, deployment, use, application, programming, training, support, and verification. Open-ended expositional and theoretical approaches that elucidate general algorithmic principles through concrete instances of governance arise from the recent proliferation of algorithmic systems and their simultaneous social implementation and institutional appreciation. Insightful yet prescriptive normative models and frameworks exist but remain better suited for initial phases of dedicated algorithmic-governance developments rather than later stages [8]. Consequently, more utilitarian presentations that frame algorithmic-governance topicality for policy consideration, professional reflection, and research inquiry predominate, with empirical examples and authoritative preliminaries complementing continuously unfolding developments [6].

Methodological Rigor in Auditing

Auditing is a well-known practice for assessing the processes, outputs, and impacts of systems of high societal stakes. A lack of rigor in defining what constitutes an audit may also lead to ineffective governance interventions in automated systems [13]. Algorithmic audits tend to focus exclusively on technical aspects rather than on how algorithms are actually used, which social contexts are relevant, or what skills users possess [15]. Correctness metrics from proprietary systems can therefore originate from configurations that no operator ever implements. In cases where algorithmic outcome monitoring occurs in practice upon system delivery, standard-checked practices do not always align with those observed post-implementation [14]. The only constraint may be that the delivered system fits into the architecture. Since various audit streams may simultaneously enforce conflicting objectives, regulatory exposure can diminish its attractiveness [1].

Data Quality and Bias Assessment

Data quality and bias assessments are fundamental constituent elements of algorithmic transparency and, by extension, algorithmic accountability [13]. Public-sector algorithmic decision-making systems have material effects on individuals and groups; the setting and implementation of rules governing the use of a system, therefore, deserve scrutiny [2]. Disclosures about the data underpinning algorithms and the parameters governing their functioning are part of due diligence [12]. Furthermore, the same elements that inform the responsible use of algorithms, even those of a certain degree of opacity, also enable public agencies and stakeholders to critically assess their functioning [13]. Officials, stakeholders, and the public benefit from understanding what information shapes an algorithm's decisions, from which the system's potential impacts and disruptive possibilities can be further unravelled [1].

Normative Frameworks and Measurement of Harm

Normative frameworks and criteria for the measurement of harm constitute a crucial input for the governance of algorithmic systems [3]. To determine whether an algorithmic system is fulfilling its public purpose and meeting pertinent constraints, it is essential to clarify what constitutes harm and the associated metrics [10]. Without clear and publicly accepted criteria, systems can continue to operate and expand without addressing significant concerns, posing risks that may not seem urgent enough to halt their deployment. As algorithmic systems grow more advanced, the potential for unforeseen and disproportionate harm also increases, rendering transparency, auditability, and participation insufficient to ensure proper oversight [11]. A more substantial risk emerging from these systems is the intensification of existing social pathologies, including discrimination, disinformation, financial fraud, and public health misinformation. Such issues are already the subject of significant debate across society, and reckoning with these difficulties in ongoing algorithm deployments can prepare for the larger and novel challenges posed by the latest advances in artificial intelligence [12]. For algorithmic governance to be effective, both analytic clarity on what constitutes a societal problem and clearly understood criteria and metrics are needed for the assessment of these systems, including those based on deep-learning technology [13].

Implementation Challenges and Best Practices

Algorithmic decision-making is impacting important and sensitive domains (e.g., social policies, criminal justice, and public health) [13]. The deployment of algorithmic systems raises challenges that need to be addressed in order to educate affected populations, promote civic oversight, enable civic engagement, and establish norms of appropriateness [1, 2]. Public actors increasingly rely on these systems due to incentivized efficiencies and alleged objectiveness. The consequential past-deployed algorithms show the importance of governance elements (e.g., audits, transparency, and harm). A democratic framework suggests the same parameters as relevant for algorithm governance mechanisms [12].

Institutional Incentives and Capacity

Algorithmic governance interacts with political accountability across many levels of government and in numerous contexts, but the prevalence of these interactions varies widely from place to place [5]. When local public capacities, such as managerial skills and technical expertise, meet the normative idea of algorithmic governance at

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

a political level in the nation or agency, local public capacities first increase and then gradually converge with national or organizational levels [14]. Holding algorithmic systems accountable requires internal resources in the relevant public administration. For a large portion of citizens, public institutions that govern algorithmic systems lack critical abilities. Developing rigorous and comprehensive statistical standards for algorithmic systems of different types requires a significant investment of time, manpower, and funds [13]. Long-standing public accountability channels, such as compliance with parliamentary oversight and access to legislation, online platforms, and public hearings applied to algorithmic audits, suffer diligence deficits and, consequently, mechanisms laid out in relevant democratic constitutions and in numerous statutes devolve into empty formalities [14]. Steps taken at the political level set off a chain of responses along the public administration hierarchy and instigate positive feedback, thereby widening gaps across the public sector [13]. An equally deliberate effort to align public audit efforts with the incentives of public institutions operating under algorithmic systems, alongside ongoing focus on strengthening technical capacities, arises as a pressing priority [2, 1].

Cross-Sector Collaboration

Government and industry are engaged in a dual dialogue about algorithmic management in automated systems. Governments propose legislation to specify algorithmic impact reporting obligations [13]. Industry proposes the AI Risk Management Framework, which recommends documenting algorithmic performance against pre-specified criteria. Abundant algorithmic analytics data would facilitate collaboration to accurately measure algorithmic risk and explain evaluation criteria, assumptions, and uncertainties. Such collaboration could extend to articulating the impact of algorithmic systems on societal challenges, including equity, fairness, and bias [5].

International Harmonization and Standards

International harmonization of standards for algorithmic systems is critical to facilitate consistent and coherent implementation of auditing, transparency, and accountability measures across jurisdictions and to help countries develop initiatives in places where public policy on algorithmic applications is still evolving [3]. Although many standard-setting organizations already offer guidance in specific domains, e.g., G20 AI Principles, OECD AI Principles, ISO/IEC TR 24028, a comprehensive international framework is needed that clarifies interrelationships among auditing, transparency, and public accountability for algorithmic systems, assesses risks and harms associated with their deployment, and provides guidance on mitigation measures [14]. Such a framework should also underline the crucial need for inclusive stakeholder engagement in standards preparation and not-for-profit participation in audits to protect democracy from potential erosion by algorithmic systems [15].

CONCLUSION

The increasing integration of algorithmic systems into public governance structures has transformed decision-making processes across a wide range of societal domains. While these technologies offer opportunities to improve efficiency, optimize resource allocation, and generate data-driven insights, they also introduce significant challenges related to fairness, transparency, and accountability. As algorithmic decision-making expands within public administration, establishing effective governance mechanisms becomes essential to ensure that these systems operate in alignment with democratic values and human rights principles. This paper has highlighted the central role of audits, transparency, and harm assessment in the governance of algorithmic systems. Algorithmic audits, whether conducted internally or by independent external actors, provide crucial tools for evaluating system performance, identifying biases, and assessing risks associated with automated decision-making. The development of standardized auditing frameworks and performance metrics is therefore necessary to ensure consistent and meaningful oversight across different sectors and jurisdictions. Transparency also plays a foundational role in enabling accountability. Mechanisms such as data provenance disclosure, model documentation, explainability techniques, and governance records provide stakeholders with insights into how algorithmic systems operate and how decisions are produced. These mechanisms enable citizens, regulators, and civil society organizations to scrutinize algorithmic practices and contest decisions that may produce unjust outcomes. Without transparency, algorithmic systems risk becoming opaque “black boxes” that undermine trust in public institutions and weaken democratic oversight. Equally important is the recognition and measurement of harm arising from algorithmic systems. Such harms may occur at multiple levels, affecting individuals, specific groups, or entire societies. Discrimination, privacy violations, economic exclusion, and erosion of public trust represent some of the most pressing risks associated with poorly governed algorithmic systems. Addressing these harms requires not only technical solutions but also strong governance frameworks that incorporate legal accountability, civic oversight, and participatory decision-making. The analysis also demonstrates that implementing algorithmic governance frameworks faces several challenges, including limited institutional capacity, insufficient technical expertise within public administrations, restricted access to proprietary data, and inconsistent regulatory standards across jurisdictions. Overcoming these challenges requires cross-sector collaboration among governments, industry

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited

actors, researchers, and civil society organizations. International cooperation and the harmonization of standards will also be critical to ensure consistent oversight and accountability for algorithmic systems deployed across borders. Ultimately, algorithmic governance must be understood as an ongoing socio-technical process rather than a one-time regulatory intervention. Continuous monitoring, transparent reporting, participatory oversight, and adaptive regulatory frameworks are necessary to keep pace with rapidly evolving technologies. By strengthening auditing practices, promoting transparency, and establishing clear pathways for addressing harm, policymakers and institutions can ensure that algorithmic systems serve the public interest while protecting democratic values, human rights, and societal well-being.

REFERENCES

1. Busuioc M. Accountable artificial intelligence: Holding algorithms to account. *Public administration review*. 2021 Sep;81(5):825-36.
2. Brauneis R, Goodman EP. Algorithmic transparency for the smart city. *Yale JL & Tech.*. 2018;20:103.
3. McGregor L, Murray D, Ng V. International human rights law as a framework for algorithmic accountability. *International & Comparative Law Quarterly*. 2019 Apr;68(2):309-43.
4. Vecchione B, Levy K, Barocas S. Algorithmic auditing and social justice: Lessons from the history of audit studies. In *Proceedings of the 1st ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization* 2021 Oct 5 (pp. 1-9).
5. Percy C, Dragicevic S, Sarkar S, d'Avila Garcez A. Accountability in AI: From principles to industry-specific accreditation. *AI Communications*. 2022 Mar 4;34(3):181-96.
6. Meßmer AK, Degeling M. Auditing Recommender Systems--Putting the DSA into practice with a risk-scenario-based approach. *arXiv preprint arXiv:2302.04556*. 2023 Feb 9.
7. Gorwa R, Ash TG. Democratic transparency in the platform society. *Social media and democracy: The state of the field and prospects for reform*. 2020 Sep 3:286-312.
8. Beckmann P, Gombert K, Hoppe A, Jautz K, Lindner M, Roome J, San Nicolás H, Schartau L, Schmälter J, Stiller T, Theunissen A. Transparency--more than a buzzword?. *MaRBL*. 2012 Jul 1;1.
9. Singh J, Cobbe J, Norval C. Decision provenance: Harnessing data flow for accountable systems. *IEEE Access*. 2018 Dec 17;7:6562-74.
10. Edwards L, Veale M. Slave to the algorithm? Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*. 2017;16:18.
11. Cooper AF, Moss E, Laufer B, Nissenbaum H. Accountability in an algorithmic society: relationality, responsibility, and robustness in machine learning. In *Proceedings of the 2022 ACM conference on fairness, accountability, and transparency* 2022 Jun 21 (pp. 864-876).
12. Shelby R, Rismani S, Henne K, Moon A, Rostamzadeh N, Nicholas P, Yilla-Akbari NM, Gallegos J, Smart A, Garcia E, Virk G. Sociotechnical harms of algorithmic systems: Scoping a taxonomy for harm reduction. In *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* 2023 Aug 8 (pp. 723-741).
13. Oduro S, Moss E, Metcalf J. Obligations to assess: Recent trends in AI accountability regulations. *Patterns*. 2022 Nov 11;3(11).
14. Jonk E, Iren D. Governance and communication of algorithmic decision making: A case study on public sector. In *2021 IEEE 23rd Conference on Business Informatics (CBI)* 2021 Sep 1 (Vol. 1, pp. 151-160). IEEE.
15. Li R, Kingsley S, Fan C, Sinha P, Wai N, Lee J, Shen H, Eslami M, Hong J. Participation and Division of Labor in User-Driven Algorithm Audits: How Do Everyday Users Work together to Surface Algorithmic Harms?. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* 2023 Apr 19 (pp. 1-19).

CITE AS: Tarcisius Niwagaba (2026). Algorithmic Governance and Public Accountability: Audits, Transparency, and Harm. NEWPORT INTERNATIONAL JOURNAL OF CURRENT ISSUES IN ARTS AND MANAGEMENT, 7(1): 10-19.
<https://doi.org/10.59298/NIJCIAM/2025/71.1019>