

GOVERNING DEEPPFAKES: A LEGAL FRAMEWORK FOR ELECTORAL INTEGRITY IN SIERRA LEONE

Thomas Sheku Marah*, Bram B. Baan, Ujang Badru Jaman

Departments of Business, Humanities and Law, Nusa Putra University, Sukabumi, West Java, Indonesia

*thomasmarah0@gmail.com

Abstract

The rapid development of generative artificial intelligence has created significant legal challenges for electoral governance through the emergence of deepfake technologies capable of producing highly realistic but fabricated political content. Unlike conventional misinformation, deepfakes generate synthetic representations of reality that challenge traditional understandings of authenticity, evidence, public trust, and democratic accountability. This study examines the adequacy of Sierra Leone's legal framework in addressing AI-generated electoral manipulation through an integrative legal research approach combining doctrinal legal analysis, comparative legal analysis, and regulatory governance analysis. The study evaluates the Constitution of Sierra Leone 1991, the Public Elections Act 2022, the Cyber Security and Crime Act 2021, and the Independent Media Commission Act 2020, while incorporating comparative perspectives from the European Union, selected United States jurisdictions, and Singapore. The findings reveal that Sierra Leone does not face a complete legal vacuum concerning deepfake-related electoral harms. Existing technology-neutral provisions may address specific forms of synthetic electoral interference where statutory requirements are satisfied. Nevertheless, the current framework remains fragmented and inadequate in regulating synthetic representation, deceptive authenticity, provenance transparency, platform accountability, and time-sensitive electoral remedies. To address these limitations, this study introduces the concept of Synthetic Electoral Manipulation (SEM) as a distinct legal category of electoral interference characterized by synthetic representation, electoral nexus, deceptive authenticity, legally relevant culpability, and democratic harm. The study further proposes a Synthetic Electoral Integrity Framework (SEIF), consisting of five pillars: Electoral Deepfake Classification System, Political AI Transparency Obligations, Platform Accountability Duties, Electoral Deepfake Offences, and Emergency Electoral Response Mechanism. This framework provides a constitutionally grounded approach that seeks to protect electoral integrity while preserving freedom of expression, due process, and democratic participation. The study contributes to emerging debates on AI governance, electoral law, and digital constitutionalism by offering a context-sensitive model for Sierra Leone and other emerging democracies confronting AI-enabled electoral manipulation.

Keywords: Deepfakes; Electoral Integrity; Artificial Intelligence Governance; Synthetic Electoral Manipulation; Digital Constitutionalism.

A. Introduction

The rapid advancement of generative artificial intelligence (AI) is fundamentally reshaping the informational foundations upon which contemporary democratic systems operate (Branford et al., 2025). Among the most disruptive manifestations of this transformation is deepfake technology, which employs sophisticated machine-learning techniques to generate highly realistic

synthetic audio, video, and visual content capable of convincingly imitating real individuals, events, and communications (Maniyal & Kumar, 2024). Unlike conventional forms of misinformation, deepfakes do not merely disseminate false information; they manufacture synthetic representations of reality that may be indistinguishable from authentic evidence (Al-Khazraji et al., 2023). Consequently, the emergence of deepfakes challenges long-standing assumptions concerning truth verification, evidentiary reliability, public trust, and democratic accountability. As political communication increasingly migrates to digitally mediated environments, the capacity of deepfakes to manipulate public perception has become a pressing legal, constitutional, and governance concern.

The significance of this challenge is particularly evident within electoral processes. Democratic elections depend upon an informational environment in which citizens can evaluate political actors, competing policy positions, and public affairs through access to reasonably reliable information (Romero et al., 2025). Electoral legitimacy is therefore inseparable from the integrity of the communication ecosystem within which democratic participation occurs (Ahmed et al., 2025). Deepfakes threaten this relationship by enabling the large-scale production of fabricated speeches, manipulated campaign messages, synthetic endorsements, and fictitious political events capable of influencing voter perceptions and electoral behavior (Pooja Raj, 2025). Unlike traditional electoral misconduct, which generally involves identifiable actors engaging in unlawful conduct, deepfakes introduce a technologically mediated form of manipulation that operates through algorithmically generated content capable of exploiting the persuasive authority historically associated with audiovisual evidence (Amezaga & Hajek, 2022). Electoral harm is therefore no longer confined to misinformation or disinformation but increasingly encompasses the construction of synthetic political realities capable of distorting democratic choice itself (Visnjic, 2025).

These developments present particularly acute challenges for emerging democracies. While advanced democracies have begun developing regulatory responses to AI-generated content, many developing states remain governed by legal frameworks designed for analogue or early-digital information environments (Hanna et al., 2026; Karanja & Nzau, 2026). Sierra Leone illustrates this challenge in a particularly significant manner. Since the conclusion of its civil conflict, the country has pursued extensive democratic and constitutional reforms aimed at strengthening political participation, electoral legitimacy, and institutional accountability (Marah, 2026b). Simultaneously, increasing internet penetration, widespread mobile-phone adoption, and growing reliance on social media platforms have transformed the structure of political communication (Sam, 2019). Electoral campaigns, civic engagement, and public deliberation increasingly occur through digital platforms that remain vulnerable to emerging forms of technological manipulation (Eskiadi & Panagiotou, 2025). The continuing process of democratic consolidation, institutional capacity constraints, and periodic electoral contestation further create conditions in which synthetic political content may generate disproportionate effects on public trust and electoral legitimacy (Shaholli, 2025). Sierra Leone therefore represents not merely a geographically convenient case study but an important example of how emerging democracies may confront the governance challenges posed by AI-generated electoral interference.

This study is informed by three complementary theoretical perspectives. First, Electoral Integrity Theory, particularly as developed by Norris (2014), emphasizes that democratic elections require more than procedural compliance; they depend upon transparency, fairness, accountability, and equal opportunities for political competition. Electoral integrity therefore extends beyond electoral administration to encompass the informational conditions under which citizens form political judgments (Norris, 2014). Second, Information Disorder Theory, developed by Wardle and Derakhshan, provides a framework for understanding how misinformation, disinformation, and malinformation disrupt democratic discourse (Wardle & Derakhshan, 2017). However, deepfakes introduce a more sophisticated form of manipulation because they combine

informational deception with synthetic audiovisual realism capable of enhancing credibility, emotional influence, and persuasive impact. Third, Digital Constitutionalism provides a normative framework for evaluating how constitutional values including democratic participation, freedom of expression, political equality, and accountability should be protected within digitally mediated public spheres. Digital Constitutionalism provides an additional normative framework for examining how constitutional principles, including fundamental rights, democratic participation, accountability, and limitations on public and private power, should operate within digitally mediated environments. De Gregorio (2022) emphasizes the emergence of constitutional responses to digital power and the need to preserve constitutional values in the governance of digital technologies, while Pollicino and Romeo (2016) highlight the challenges posed by digital environments to the protection and interpretation of fundamental rights. Collectively, these theoretical approaches provide an analytical foundation for assessing whether existing legal frameworks remain capable of safeguarding electoral integrity in the age of generative artificial intelligence.

Existing scholarship has generated significant insights into the relationship between digital technologies and democratic governance. Research on election misinformation and digital propaganda demonstrates how false information can influence political attitudes, reinforce polarization, and undermine public trust in democratic institutions. Studies by Vaccari and Chadwick (2020) show that digitally mediated political communication increasingly operates through hybrid information environments in which misinformation and manipulation can spread rapidly across platforms. Similarly, scholarship on deepfake governance by Chesney and Citron (2019) identifies the unique risks posed by synthetic media for democratic legitimacy, reputational integrity, and information authenticity. Research by Paris and Donovan (2019) and Westerlund (2019) further demonstrates that synthetic media technologies challenge conventional assumptions regarding the authenticity, credibility, and social trust associated with audiovisual communication. By enabling the creation of highly realistic but fabricated images, audio, and videos, deepfake technologies undermine the traditional perception of audiovisual materials as reliable representations of reality and create new challenges for public verification and information integrity.

Parallel debates have emerged within the broader literature on artificial intelligence governance and platform regulation. Floridi et al. (2018) emphasize the importance of transparency, accountability, and human-centred approaches in governing artificial intelligence systems and addressing the ethical challenges associated with emerging technologies. Similarly, Helberger (2020) highlights the increasing role of digital platforms and algorithmic systems in shaping the conditions of contemporary democratic communication, including the visibility and circulation of political information. Scholarship on platform governance further demonstrates that democratic discourse is increasingly mediated by privately operated digital infrastructures whose design choices, content moderation practices, and algorithmic processes influence the dissemination and amplification of political content. Collectively, these studies illustrate that AI-generated content cannot be understood solely as an informational problem but also as a broader governance challenge involving transparency, accountability, platform power, and the protection of democratic processes.

Nevertheless, existing scholarship remains divided concerning the appropriate legal response to deepfake technologies. One strand of literature conceptualizes deepfakes primarily as a subset of misinformation, disinformation, cybercrime, defamation, or platform-governance problems. From this perspective, existing legal frameworks can be adapted to address deepfake-related harms without substantial conceptual innovation. A second strand argues that the unprecedented capabilities of generative AI require entirely new regulatory approaches because synthetic media fundamentally alters established assumptions concerning authenticity, evidence, and accountability.

While both perspectives contribute important insights, neither fully captures the distinctive legal character of deepfake-driven electoral interference. The first approach underestimates the extent to which synthetic media transforms the nature of electoral deception, while the second frequently focuses on technological governance without adequately conceptualizing the specific legal harms that deepfakes create within democratic processes. Consequently, existing scholarship has not sufficiently developed a legal theory explaining why AI-generated synthetic media should be understood as a distinct category of electoral harm requiring separate legal recognition. This limitation is particularly evident within emerging democracies, where the interaction between electoral governance, constitutional rights, platform regulation, and AI-generated political communication remains significantly underexplored.

This article addresses that gap by advancing a third position. It argues that deepfakes constitute a distinct form of electoral interference that cannot be adequately understood through existing categories of misinformation, cybercrime, or electoral misconduct. To capture this phenomenon, the article introduces the concept of Synthetic Electoral Manipulation (SEM), defined as electoral interference conducted through AI-generated audiovisual content designed to distort political perception, influence voter judgment, or undermine confidence in democratic processes through the creation of synthetic political realities. Crucially, SEM is proposed not merely as a technological category but as a legally cognizable form of electoral interference constituted by five interrelated elements: (1) a synthetic-representation element, involving AI-generated or materially AI-manipulated audiovisual content that falsely represents a person, institution, statement, endorsement, or political event; (2) an electoral-nexus element, requiring a sufficiently direct connection between the synthetic content and an electoral process, campaign, candidate, voter participation, or electoral institution; (3) a deceptive-authenticity element, whereby the representation is presented, or is reasonably capable of being perceived, as authentic rather than transparently fictional or synthetic; (4) a culpability element, particularly where criminal or punitive liability is contemplated, requiring intentional or knowing deployment of the synthetic representation for electoral influence, voter suppression, fabricated endorsement, reputational manipulation, or disruption of electoral confidence; and (5) a democratic-harm element, requiring actual harm or a material risk of harm to informed voter choice, political equality, electoral participation, institutional trust, or the integrity of electoral competition. These elements distinguish SEM not simply by the use of AI, but by the convergence of synthetic authenticity, electoral connection, deceptive deployment, legally relevant culpability, and democratic harm. They also establish principled boundaries around the concept: transparently labelled synthetic content, satire, parody, artistic expression, legitimate journalism, research, and other constitutionally protected uses should not fall within SEM merely because AI-generated material is involved. By conceptualizing deepfake-driven electoral interference as a distinct legal category, the article provides a new analytical framework for understanding the relationship between generative AI and electoral integrity.

The article is correspondingly limited to the legal governance of AI-generated or materially AI-manipulated synthetic audiovisual content that bears a demonstrable electoral nexus. It does not attempt to regulate generative AI generally, nor does it treat all misinformation, ordinary political falsehoods, defamation, cybercrime, or non-electoral synthetic media as falling within the scope of SEM. Empirically, Sierra Leone constitutes the focal jurisdiction, while the European Union, selected United States jurisdictions, and Singapore are used only as comparative regulatory reference points from which analytically transferable principles may be identified rather than as functionally equivalent legal systems.

Within this delimited scope, the study addresses two research questions: (1) To what extent do Sierra Leone's existing constitutional, electoral, cybercrime, and media laws regulate the constitutive legal elements and democratic harms associated with Synthetic Electoral Manipulation? (2) What constitutionally constrained regulatory architecture, informed by

comparative developments in the European Union, selected United States jurisdictions, and Singapore, can address the identified legal and institutional gaps while preserving freedom of expression, due process, proportionality, and electoral integrity?

Accordingly, this study seeks to develop a legal framework capable of protecting electoral integrity from deepfake-generated electoral manipulation in Sierra Leone. Through the integration of Electoral Integrity Theory, Information Disorder Theory, and Digital Constitutionalism, the article examines the limitations of existing legal instruments and develops a Synthetic Electoral Integrity Framework (SEIF) designed to address emerging forms of AI-driven electoral interference. The inquiry therefore proceeds from legal characterization to regulatory adequacy and, finally, to institutional design: it first determines what legally constitutes SEM, then evaluates whether Sierra Leone's existing framework addresses those constitutive elements, and subsequently develops SEIF as a context-sensitive response to the deficiencies identified through doctrinal and comparative analysis. The significance of this study lies not only in its contribution to contemporary debates on AI governance, electoral law, and digital constitutionalism but also in its development of a theory-informed governance framework capable of assisting emerging democracies in responding to the challenges posed by synthetic political communication.

This study employs Integrative Legal Research combining doctrinal legal analysis, comparative legal analysis, and regulatory governance analysis to examine the legal implications of AI-generated synthetic media within electoral processes and to develop a constitutionally grounded framework for addressing Synthetic Electoral Manipulation (SEM) in Sierra Leone. An integrative design is appropriate because synthetic electoral manipulation does not fall exclusively within a single legal field; rather, it intersects constitutional law, electoral law, cybercrime regulation, media governance, platform accountability, and artificial intelligence governance. The analysis therefore moves beyond identifying whether existing legislation expressly refers to artificial intelligence or deepfakes. It evaluates whether existing technology-neutral legal rules can regulate particular manifestations of SEM, the conditions under which those provisions apply, the residual regulatory functions they do not perform, and the constitutional limits governing any proposed legal response. This approach enables the study to assess substantive legal coverage, regulatory coherence, institutional and remedial capacity, and constitutional legitimacy within a single analytical framework.

The doctrinal component systematically identifies, interprets, and evaluates the primary legal rules governing political communication, electoral participation, electoral misconduct, cyber-enabled interference, and media regulation in Sierra Leone. The principal domestic materials comprise the Constitution of Sierra Leone 1991, the Public Elections Act 2022, the Cyber Security and Crime Act 2021, the Independent Media Commission Act 2020, the Independent Media Commission (Print and Electronic Media) Regulations 2022, relevant subsidiary legislation, and applicable regulatory instruments concerning the administration of elections. The Constitution provides the primary normative benchmark, particularly through Section 25 on freedom of expression and Sections 31–36 concerning voting, electoral administration, and the constitutional position of the Electoral Commission. Digital Constitutionalism is used as a supporting interpretive framework rather than as an independent source of constitutional authority. Secondary materials comprise peer-reviewed journal articles, scholarly monographs, legal commentaries, policy reports, and relevant international and comparative regulatory materials concerning electoral integrity, information disorder, synthetic media, platform governance, and artificial intelligence regulation.

The doctrinal inquiry does not infer regulatory inadequacy merely from the absence of AI-specific terminology. Instead, potentially applicable technology-neutral provisions are subjected to an element-by-element legal analysis before any regulatory gap is identified. In particular, provisions concerning personation, false statements, undue influence, wrongful voting, electoral interference, computer-related forgery and fraud, identity-related offences, and media

responsibilities are examined according to their legally required conduct, mental element, electoral connection, protected interest, and available remedies. Their scope is then assessed against the five constitutive elements of SEM developed in this study: synthetic representation, an electoral nexus, deceptive authenticity, legally relevant culpability, and actual or materially foreseeable democratic harm. This analytical structure distinguishes between: (1) direct legal coverage, where the elements of an existing provision correspond to the relevant synthetic electoral conduct; (2) conditional or technology-neutral coverage, where an existing rule may apply only if its independent statutory elements are established; and (3) a residual regulatory gap, where no existing rule adequately performs the regulatory function under examination. The concept of regulatory inadequacy is therefore used to denote incomplete, fragmented, or functionally mismatched legal coverage rather than a complete legal vacuum.

To complement the domestic doctrinal analysis, the study employs a purposive comparative legal method. Comparative jurisdictions were selected according to functional relevance and analytical transferability, rather than institutional similarity, geographic representativeness, or an assumption that foreign regulatory models are inherently superior to Sierra Leonean law. The European Union was selected because its Artificial Intelligence Act and Digital Services Act provide identifiable mechanisms concerning synthetic-content transparency, provenance, platform systemic-risk assessment, and intermediary accountability. Within the United States, the analysis is deliberately limited to California, Minnesota, and Washington, which illustrate distinct approaches to election-specific synthetic-media regulation through disclosure, criminal, civil, and injunctive mechanisms. Singapore was selected because its electoral and online-content governance framework provides an analytically relevant example of election-specific regulation of digitally manipulated candidate representations together with comparatively rapid corrective mechanisms. These jurisdictions therefore supply different regulatory functions that can be evaluated against the deficiencies identified within Sierra Leone's legal framework; they are not treated as functionally equivalent constitutional systems or as models for direct legal transplantation.

The comparative analysis is conducted through a common functional matrix to avoid impressionistic jurisdictional comparison. Each jurisdiction is evaluated according to four predetermined criteria: legal specificity, referring to whether legislation expressly recognizes synthetic, deepfake, or digitally manipulated content; electoral specificity, assessing whether the relevant rule is directly connected to candidates, campaigns, political advertising, voting, or a defined electoral period; regulatory reach, examining whether obligations apply only to content creators or also extend to platforms, intermediaries, and other institutional actors; and remedial capacity, assessing the availability of disclosure, correction, disabling, civil, criminal, injunctive, or expedited remedies. Comparative classifications are consequently functional rather than evaluative. "Explicit" denotes direct statutory recognition of synthetic or manipulated content; "technology-neutral/conditional" denotes potential coverage dependent upon satisfaction of an existing general provision; "jurisdiction-specific" denotes regulatory coverage limited to particular subnational jurisdictions; and "no dedicated mechanism" indicates that no identified rule specifically performs the regulatory function being assessed. This coding structure provides the methodological basis for the comparative assessment presented in the Results and Discussion.

The collected legal materials are analyzed through a sequential four-stage process. First, doctrinal interpretation identifies the content, scope, elements, limitations, and remedies associated with Sierra Leone's constitutional, electoral, cybercrime, and media provisions. Particular attention is given to whether existing technology-neutral provisions already regulate components of SEM before any claim of legal deficiency is made. Second, the domestic framework is evaluated across four interrelated dimensions: constitutional compatibility, assessing consistency with the rights, institutions, and limitations contained principally in the Constitution of Sierra Leone; substantive coverage, examining the degree to which existing provisions capture the five elements of SEM;

regulatory and institutional coherence, evaluating interactions and potential gaps among electoral, cybercrime, media, and platform-governance regimes; and remedial responsiveness, examining whether available institutional powers and legal remedies can address synthetic electoral harms within electorally consequential timeframes. Third, the comparative analysis applies the common functional criteria described above to the European Union, California, Minnesota, Washington, and Singapore to identify regulatory mechanisms corresponding to residual deficiencies established through the Sierra Leonean doctrinal analysis. Fourth, the doctrinal and comparative findings are interpreted through Electoral Integrity Theory, Information Disorder Theory, and Digital Constitutionalism. Electoral Integrity Theory identifies the democratic interests threatened by synthetic interference; Information Disorder Theory explains the production, circulation, and amplification of deceptive synthetic content; and Digital Constitutionalism provides a supporting normative framework for assessing legal certainty, proportionality, transparency, rights protection, and institutional accountability in digitally mediated electoral governance.

The Synthetic Electoral Integrity Framework (SEIF) is developed through a structured two-stage synthesis rather than through abstract policy prescription. At the first stage, the doctrinal analysis identifies a residual regulatory function that Sierra Leone's existing legal framework does not adequately perform after all potentially applicable technology-neutral provisions have been examined. At the second stage, comparative analysis determines whether one or more selected jurisdictions employ an identifiable mechanism performing that function. The transferable regulatory principle is then adapted to Sierra Leone's constitutional and institutional context and evaluated against the theoretical perspectives employed in the study. Each SEIF pillar must therefore satisfy a traceable derivation sequence linking the identified domestic doctrinal deficiency to a corresponding comparative governance function, then to the relevant theoretical and constitutional constraints, and finally to a context-specific regulatory response. This process generates five corresponding pillars: deficiencies in distinguishing harmful synthetic deception from protected expression support the Electoral Deepfake Classification System; the absence of dedicated provenance and disclosure mechanisms supports Political AI Transparency Obligations; the absence of systemic election-period intermediary responsibilities supports Platform Accountability Duties; the incomplete fit between existing offences and the integrated elements of SEM supports narrowly defined Electoral Deepfake Offences; and the absence of a dedicated time-sensitive remedy supports an Emergency Electoral Response Mechanism. Comparative law thus informs regulatory design without displacing Sierra Leone's constitutional framework or presuming the direct transferability of foreign institutions.

Constitutional legitimacy is assessed principally through the Constitution of Sierra Leone. The study does not assume the existence of an autonomous constitutional right to "electoral authenticity." Instead, it evaluates whether a derivative constitutional interest in electoral authenticity can be normatively justified through the interaction of existing protections for political expression, voting, electoral participation, and independent electoral administration. Any proposed SEM regulation is consequently assessed according to legality, legitimate constitutional purpose, precision of the regulated conduct, necessity, proportionality, procedural fairness, institutional independence, and availability of effective judicial review. This constitutional analysis is particularly important for classification, liability, platform intervention, and emergency measures because measures intended to protect electoral integrity may themselves threaten freedom of expression or facilitate politically motivated restrictions if drafted or implemented too broadly.

The study is subject to limitations inherent in its integrative legal design. It does not empirically measure voter susceptibility to deepfakes, the prevalence of synthetic electoral content in Sierra Leone, the operational practices of digital platforms, or the actual enforcement performance of electoral, cybersecurity, and media institutions. Nor does the comparative analysis establish that mechanisms adopted in the European Union, selected United States jurisdictions, or Singapore would produce equivalent outcomes if introduced in Sierra Leone. SEIF should

therefore be understood as a normative and institutionally informed legal governance framework whose practical effectiveness remains an empirical question. Nevertheless, the systematic combination of element-by-element doctrinal analysis, functionally structured comparative analysis, explicit constitutional evaluation, and transparent framework derivation provides a rigorous methodological basis for identifying regulatory incompleteness and developing context-sensitive legal responses to AI-enabled electoral manipulation.

B. Discussion

1. Deepfakes and the Transformation of Electoral Harm

Electoral law has historically evolved around the regulation of human-generated misconduct (Edwards, 2019). Traditional legal frameworks governing elections were developed to address identifiable forms of interference such as voter intimidation, electoral fraud, campaign finance violations, political defamation, dissemination of false statements, and other forms of unlawful influence exercised by individuals, organizations, or political actors (Van De Velde, 2021). Although these forms of misconduct vary in nature and severity, they share a common assumption: electoral harm originates from human conduct occurring within an informational environment in which the authenticity of political communication is generally presumed (Luebke, 2021). Consequently, electoral regulation has traditionally focused on controlling deceptive behavior rather than questioning the reliability of political reality itself.

The emergence of generative artificial intelligence fundamentally disrupts this assumption. Deepfake technologies enable the creation of highly realistic but entirely fabricated audiovisual content capable of simulating political candidates, public officials, journalists, electoral institutions, and political events with unprecedented accuracy (Chesney & Citron, 2019). Unlike conventional misinformation, which typically relies upon false narratives, manipulated statistics, misleading claims, or deceptive textual content, deepfakes create synthetic representations that exploit the evidentiary authority historically associated with visual and auditory media (Paris & Donovan, 2019). The resulting harm extends beyond informational falsity because deepfakes are capable of manufacturing alternative versions of reality that appear authentic to ordinary citizens. Electoral deception therefore increasingly operates not through false statements alone but through algorithmically generated simulations of political reality (Kopecky, 2024).

This distinction is significant because contemporary scholarship frequently analyzes deepfakes through the broader frameworks of misinformation, disinformation, or information disorder. Information Disorder Theory has contributed substantially to understanding how misleading information circulates through misinformation, disinformation, and malinformation (Puccinelli, 2025). However, these categories primarily focus on the falsity, intent, and dissemination of information rather than the technological production of synthetic realities (Bruno & Moriggi, 2025). Disinformation, for example, generally refers to deliberately false information disseminated to deceive audiences (Marah, 2026a). Deepfakes differ in a fundamental respect (Khanjani et al., 2023). Their persuasive power does not derive solely from the falsity of information but from their ability to simulate authenticity through synthetic audiovisual representation. The legal and democratic significance of deepfakes therefore lies not merely in what they communicate but in how they reconstruct perceptions of reality itself.

Recent regulatory developments illustrate this distinction. Within the European Union, concerns surrounding AI-generated political content contributed to the adoption of transparency-oriented obligations under the AI Act and the Digital Services Act, reflecting recognition that synthetic media creates governance challenges extending beyond conventional misinformation (Steinebach et al., 2026). Similarly, several states within the United States have enacted election-specific deepfake legislation addressing synthetic political content distributed during electoral periods, acknowledging that existing misinformation and campaign regulations may be

insufficient to address AI-generated impersonation (Diakopoulos & Johnson, 2021). Singapore's regulatory approach to online falsehoods and digital content governance likewise demonstrates increasing concern with technologically amplified forms of deception that can undermine public trust and democratic processes (Jayakumar et al., 2021). Although these jurisdictions employ different regulatory strategies, each implicitly recognizes that synthetic media introduces risks that are not fully captured by traditional understandings of misinformation alone.

The inadequacy of existing categories becomes clearer when deepfakes are compared with conventional misinformation. As shown in **Table 1**, deepfakes possess characteristics that distinguish them from traditional forms of electoral deception and therefore justify separate legal treatment. The comparison also demonstrates that the regulatory distinction cannot rest solely upon the technological means by which content is generated. The legally relevant distinction concerns the interaction between synthetic representation, deceptive authenticity, an electoral nexus, culpable deployment, and a resulting threat to constitutionally protected democratic interests.

Table 1.
Distinguishing Misinformation from Synthetic Electoral Manipulation

Dimension	Traditional Misinformation	Synthetic Electoral Manipulation (SEM)
Nature of harm	False or misleading information	Artificial construction of political reality
Medium	Primarily textual or image-based	Predominantly AI-generated audiovisual content
Source	Human-generated content	Algorithmically generated or materially AI-manipulated content
Mechanism of influence	Persuasion through information	Reality simulation through synthetic representation
Primary risk	Informational distortion	Epistemic disruption and democratic manipulation
Regulatory focus	Truthfulness of information	Authenticity of political communication
Protected legal interest	Accuracy and reliability of electoral information	Effective electoral participation, authentic democratic deliberation, electoral integrity, and constitutionally protected political communication

Source: Author's conceptualization based on Electoral Integrity Theory, Information Disorder Theory, Digital Constitutionalism, and the constitutional framework governing electoral participation in Sierra Leone.

The distinction identified in **Table 1** demonstrates that deepfakes generate a form of harm that may be described as epistemic harm. Epistemic harm arises when citizens lose the ability to reliably distinguish authentic political communication from fabricated representations. Unlike conventional misinformation, which seeks to persuade citizens through false information, deepfakes undermine the evidentiary foundations upon which democratic decision-making depends. The resulting threat extends beyond individual deception and affects collective confidence in electoral processes, public institutions, and democratic discourse. In this sense, deepfakes do not merely distort information; they destabilize the conditions necessary for determining what constitutes political reality within democratic societies.

For legal purposes, however, epistemic harm cannot remain an abstract sociological or informational concept. Its relevance arises when the degradation of informational authenticity interferes with interests already protected by constitutional and electoral law. In Sierra Leone, Section 25 of the Constitution protects freedom of expression and the freedom to receive and communicate ideas and information, while Sections 31–33 establish the constitutional architecture of electoral participation and electoral administration, and Section 36 protects secret voting as an

essential condition of democratic choice (Constitution of Sierra Leone, 1991). Read together, these provisions do not create an autonomous constitutional right to a perfectly truthful or epistemically uncontaminated political sphere. They nevertheless establish protected interests in meaningful political communication, effective electoral participation, and the institutional integrity of elections. Where synthetic audiovisual content is deliberately presented as authentic in order to fabricate candidate speech, suppress participation, falsify political endorsement, impersonate electoral institutions, or materially distort voter judgment, the resulting epistemic disruption becomes legally relevant because it may impair the conditions under which those constitutional interests can be effectively exercised.

The protected interest implicated by SEM is therefore best conceptualized as electoral authenticity: not a freestanding entitlement to governmental verification of political truth, but a derivative constitutional interest in preserving the minimum informational conditions necessary for meaningful electoral choice and authentic democratic deliberation. This formulation is deliberately narrower than a generalized right to truthful political information. It distinguishes legally cognizable electoral harm from ordinary political exaggeration, contested opinion, satire, parody, and other protected forms of expression by requiring a demonstrable connection between synthetic deception and the integrity of electoral participation or competition. Epistemic harm becomes a matter for electoral law, on this account, not whenever political information is inaccurate, but when deceptive synthetic authenticity creates a sufficiently direct risk to protected democratic interests.

To address this conceptual deficiency, this article introduces the concept of Synthetic Electoral Manipulation (SEM). SEM refers to electoral interference conducted through AI-generated audiovisual content designed to distort political perception, influence voter judgment, or undermine confidence in democratic processes through the creation of synthetic political realities. SEM is not simply a technologically advanced form of disinformation. Whereas disinformation focuses on the intentional dissemination of false information, SEM focuses on the deliberate construction of fabricated representations that simulate authenticity and thereby manipulate democratic perception. The defining characteristic of SEM is therefore not informational falsity but synthetic authenticity. Consistent with the legal definition developed in this study, SEM becomes legally cognizable through the convergence of five elements: synthetic representation, a demonstrable electoral nexus, deceptive authenticity, legally relevant culpability, and actual or materially foreseeable democratic harm. The presence of AI technology alone is therefore insufficient. The concept targets synthetic content where its mode of creation, presentation, electoral connection, mental element, and capacity to impair protected democratic interests combine to produce a distinct form of electoral interference. This distinction shifts the legal focus from false information toward algorithmically manufactured political reality and provides a more precise analytical framework for understanding the harms associated with deepfake technologies.

Viewed through the lens of Electoral Integrity Theory, SEM directly threatens the informational conditions necessary for free and fair elections by contaminating the environment within which electoral choices are formed. From the perspective of Information Disorder Theory, SEM represents an intensified and technologically sophisticated form of electoral deception in which synthetic realism substantially amplifies persuasive capacity and social reach. Digital Constitutionalism further highlights how AI-generated political content challenges constitutional commitments to democratic participation, political equality, electoral fairness, and informed citizenship within digitally mediated public spheres. The three theoretical perspectives perform distinct but complementary analytical functions. Electoral Integrity Theory identifies the democratic interest threatened by synthetic interference; Information Disorder Theory explains the mechanisms through which deceptive synthetic content corrupts the informational environment; and Digital Constitutionalism supplies the normative constraints that determine when and how regulatory intervention may legitimately protect electoral authenticity without disproportionately

restricting political expression (Celeste, 2025; Jumhadi & Dewi Heniarti, 2025; Wardle & Derakhshan, 2017). Collectively, these perspectives suggest that deepfakes should not be understood merely as an extension of misinformation but as a qualitatively distinct category of electoral interference requiring specialized legal recognition.

Accordingly, this study argues that existing legal frameworks remain conceptually underdeveloped because they continue to regulate deepfakes through categories designed for human-generated information disorders. Such approaches fail to capture the unique harms associated with synthetic political realities, including epistemic disruption, algorithmic impersonation, and the erosion of public confidence in authentic political communication. More specifically, conventional categories tend to regulate isolated dimensions of the conduct falsehood, impersonation, unlawful access, defamatory content, or campaign misconduct without addressing the integrated legal configuration produced when synthetic authenticity is strategically deployed within an electoral process. SEM therefore identifies the regulatory object that falls between these established categories while simultaneously defining the conditions under which specialized legal intervention is justified. Recognizing Synthetic Electoral Manipulation as a distinct category of electoral harm is therefore not merely a matter of legal classification but a necessary step toward developing regulatory frameworks capable of safeguarding electoral integrity in the age of generative artificial intelligence.

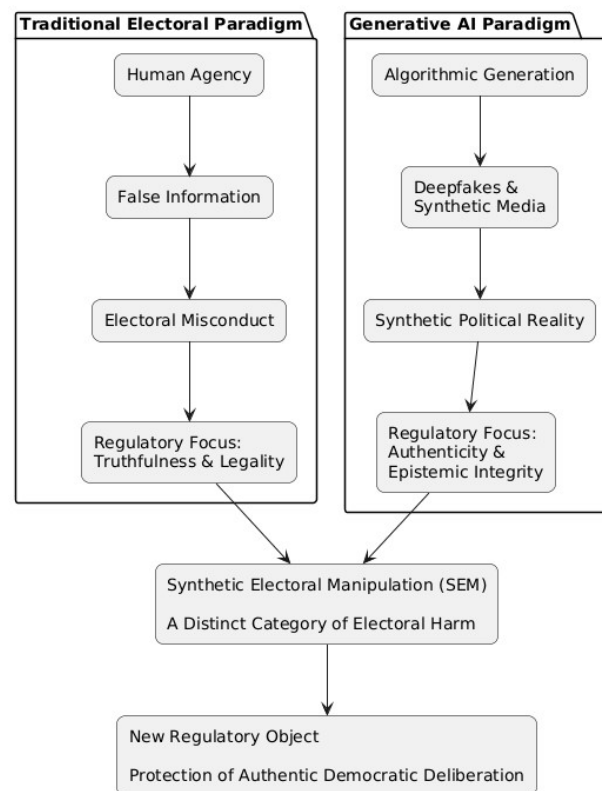


Figure 1. Conceptual Shift from Traditional Electoral Harm to Synthetic Electoral Manipulation

Source: Author's own conceptualization based on Norris (2014), Wardle and Derakhshan (2017), De Gregorio (2022), and the comparative legal analysis conducted in this study.

Figure 1 conceptualizes the transformation of electoral harm introduced by generative artificial intelligence. Rather than depicting a sequential process, the figure contrasts the assumptions underlying traditional electoral regulation with the characteristics of AI-enabled electoral manipulation and illustrates how this transformation gives rise to Synthetic Electoral

Manipulation (SEM) as a distinct regulatory object. The figure should therefore be read as a conceptual comparison between two regulatory paradigms rather than as a claim that all AI-generated political communication constitutes SEM. Only synthetic political communication satisfying the constitutive legal elements identified above enters the SEM regulatory category.

2. Assessing the Regulatory Adequacy of Sierra Leone's Existing Electoral Framework

The preceding discussion established that deepfakes constitute a distinct category of electoral harm conceptualized in this study as Synthetic Electoral Manipulation (SEM). The critical legal question is therefore whether Sierra Leone's existing constitutional and statutory framework possesses the normative and institutional capacity to regulate such conduct. This inquiry must begin with the operative electoral legislation. The Public Elections Act 2022 (Act No. 17 of 2022) repealed and replaced the Public Elections Act 2012 and therefore constitutes the principal statutory framework for the present analysis (Public Elections Act, 2022). An integrative examination of the Constitution of Sierra Leone (1991), the Public Elections Act 2022, the Cyber Security and Crime Act 2021, the Independent Media Commission Act 2020, and the Independent Media Commission (Print and Electronic Media) Regulations 2022 demonstrates that Sierra Leone does not confront a complete legal vacuum in relation to AI-generated electoral deception. Several technology-neutral provisions are potentially capable of reaching particular manifestations of SEM where their constituent statutory elements are satisfied. The more precise deficiency is one of fragmented and contingent coverage: existing provisions regulate particular consequences of synthetic manipulation such as personation, false statements, undue influence, cyber-enabled impersonation, or professional media misconduct without comprehensively addressing synthetic authenticity as an electoral regulatory object. This distinction is important because regulatory inadequacy cannot be inferred merely from the absence of the words "artificial intelligence" or "deepfake" in existing legislation.

Accordingly, legal adequacy is assessed against the five constitutive elements of SEM developed in this study: synthetic representation, electoral nexus, deceptive authenticity, culpability, and democratic harm. Existing provisions are treated as providing direct coverage where their elements expressly correspond to the conduct in question; conditional coverage where technology-neutral rules may apply only if additional statutory elements are established; and a residual regulatory gap where no existing rule adequately addresses the relevant SEM function. **Table 2** applies this approach rather than treating the absence of AI-specific terminology as synonymous with non-regulation.

Table 2.
Technology-Neutral Coverage and Residual Gaps Relating to Synthetic Electoral Manipulation in Sierra Leone

SEM-related conduct	Public Elections Act 2022	Cyber Security and Crime Act 2021	IMC Act 2020 and 2022 Regulations	Coverage assessment
AI-generated candidate impersonation	Section 123 personation protects electoral identity in the voting process but does not automatically extend to synthetic representation of a candidate's speech or conduct	Section 42 may apply where statutory identity-theft or impersonation elements are independently established	General professional and content standards may apply to regulated media	Conditional coverage; no election-specific rule directed at synthetic candidate impersonation as such
False candidate withdrawal or specified electoral falsehood communicated	Section 126 on wrongful voting and false statements may apply where the synthetic content	Potentially applicable where separate forgery, fraud, or impersonation	General standards may govern publication by	Potential substantive coverage of some deepfakes, but not a general rule

SEM-related conduct	Public Elections Act 2022	Cyber Security and Crime Act 2021	IMC Act 2020 and 2022 Regulations	Coverage assessment
through a deepfake	communicates a falsehood falling within the statutory prohibition and the relevant mental and electoral-purpose elements are proved	elements are satisfied	regulated media actors	governing deceptive synthetic political representations
Deepfake used for voter suppression or coercive electoral interference	Section 122 on undue influence may be engaged where synthetic deception operates as a means of interfering with the free exercise of the franchise and the statutory requirements are satisfied	Potential application depends on whether the conduct also constitutes a cyber offence	Indirect content-governance relevance	Technology-neutral protection exists, but application to synthetic voter suppression remains fact- and element-dependent
Fabricated speeches, endorsements, or political events	Campaign and false-statement provisions may capture particular cases, depending on content and purpose	Conditional application where conduct additionally satisfies forgery, fraud, or impersonation requirements	Professional media obligations may apply within the Commission's regulatory sphere	Fragmented coverage; no general provenance or synthetic-authenticity rule
Algorithmic amplification of electoral deepfakes by online platforms	No dedicated election-period systemic-risk or platform due-diligence duty	Offender- and computer-misuse provisions do not themselves establish a comprehensive platform-governance regime	Media regulation does not establish an equivalent election-specific systemic-risk framework for global online platforms	Structural platform-governance gap
Disclosure or provenance of AI-generated campaign material	No dedicated election-specific synthetic-content disclosure requirement identified	No general electoral AI-labelling requirement	No comprehensive election-specific provenance regime equivalent to dedicated synthetic-media disclosure rules	Transparency gap

Source: Author's doctrinal analysis of the Constitution of Sierra Leone (1991), Public Elections Act 2022, Cyber Security and Crime Act 2021, Independent Media Commission Act 2020, and Independent Media Commission (Print and Electronic Media) Regulations 2022.

Table 2 demonstrates a materially different proposition from the claim that Sierra Leone has no law capable of addressing deepfakes. The statutory framework contains technology-neutral rules that may reach discrete manifestations of SEM. Its weakness lies instead in the mismatch between the elements around which those offences were constructed and the integrated structure of synthetic electoral manipulation. The relevant question is therefore not whether existing law mentions AI, but whether its *actus reus*, mental element, protected interest, electoral nexus, and available remedies encompass the conduct generated by synthetic political communication.

At the constitutional level, the Constitution of Sierra Leone establishes the normative foundations of democratic governance through protections relating to freedom of expression,

political participation, electoral representation, and electoral administration (Constitution of Sierra Leone, 1991). Section 25 guarantees freedom of expression, including the freedom to receive and impart ideas and information, while Section 31 protects the right of eligible citizens to vote. Sections 32 and 33 establish the Electoral Commission and confer upon it responsibility for conducting and supervising voter registration, public elections, and referenda, while Section 36 requires voting by secret ballot (Constitution of Sierra Leone, 1991). These provisions perform two functions in the present analysis. First, they identify the constitutional interests potentially impaired by SEM: political communication, meaningful electoral participation, electoral administration, and the free exercise of the franchise. Second, they constrain the regulatory response because protection of electoral authenticity cannot justify disproportionate interference with political expression. The Constitution therefore supplies the normative basis for regulating serious synthetic electoral interference, but it does not itself establish an AI-specific electoral offence. That absence is not, without more, evidence of constitutional inadequacy; constitutions ordinarily articulate rights, institutional competences, and governing principles rather than technologically specific offences.

The decisive doctrinal analysis therefore concerns the Public Elections Act 2022. Unlike an approach that searches only for the terms “AI” or “deepfake,” this study examines whether its technology-neutral electoral offences can accommodate the five SEM elements. Three sets of provisions are particularly relevant: personation, false statements, and interference with the free exercise of electoral choice (Public Elections Act, 2022).

First, Section 123 addresses personation. The legal object of the offence is electoral identity within the voting process: personation concerns the fraudulent assumption of another person's identity for purposes connected with the exercise of the franchise (Constitution of Sierra Leone, 1991; Slater & Watt, 2015). This statutory conception corresponds with traditional electoral personation, where one individual presents himself or herself as another elector or otherwise attempts to exercise another person's voting entitlement. The provision is technologically neutral in the sense that technology could potentially be used as an instrument for committing or facilitating such conduct. Nevertheless, the *actus reus* does not automatically encompass a different form of impersonation in which an AI system fabricates a video or audio recording depicting a candidate as saying or doing something that never occurred. A person who disseminates a synthetic video falsely portraying a presidential candidate announcing withdrawal, endorsing an opponent, or making an inflammatory statement has created a false representation of the candidate, but has not for that reason alone assumed another voter's identity for the purpose of voting. The gap is therefore functional rather than technological: Section 123 protects the authenticity of electoral identity at the point of voting, whereas SEM may attack the authenticity of political identity and communication before a vote is cast (Constitution of Sierra Leone, 1991).

Second, Section 126, addressing wrongful voting and false statements, requires a more differentiated assessment. Unlike personation, a technology-neutral false-statement offence may encompass synthetic media because the medium through which a prohibited falsehood is communicated need not determine liability. Where, for example, an AI-generated audiovisual representation is used to communicate a false statement concerning a candidate's withdrawal and the remaining statutory requirements are satisfied, the fact that the statement was generated through AI should not by itself remove the conduct from the provision's scope. This demonstrates precisely why the absence of an express reference to deepfakes cannot be equated with non-regulation. Yet Section 126 does not thereby become a general prohibition on every deceptive synthetic representation. Its reach remains determined by the categories of false statement, culpability, electoral purpose, and other elements prescribed by the statute. A fabricated endorsement, synthetic depiction of misconduct, falsified institutional announcement, or manipulated audiovisual event may therefore fall outside Section 126 where the content does not

correspond to the particular statutory falsehood being regulated. The residual gap concerns the legal significance of deceptive synthetic authenticity, not falsity in the abstract.

Third, Section 122 on undue influence provides another technology-neutral route through which particular forms of SEM may potentially be addressed. Where a deepfake is deliberately used to prevent, impede, or improperly influence the free exercise of the electoral franchise for example, through fabricated communications designed to induce voters not to participate the synthetic medium does not necessarily prevent the application of an offence framed around unlawful electoral influence. Application would nevertheless depend upon proof of the statutory conduct, requisite culpability, connection with electoral choice, and causal or purposive relationship required by the provision. Accordingly, a voter-suppression deepfake may fall within existing law in circumstances where a merely reputational or satirical synthetic representation would not.

The wider architecture of the 2022 Act reinforces this conclusion. Its electoral-offence provisions regulate interference with election materials, lawful political meetings, free political canvassing and campaigning, disorderly electoral conduct, wrongful voting, and election-day misconduct, while its information-technology provisions beginning at Section 138 address unauthorized access and modification of computer material. Part XIV further regulates the election campaign period, campaign materials, publication of information, campaign conduct, and related obligations. These provisions demonstrate that the Act is neither exclusively analogue nor wholly incapable of responding to technology-mediated misconduct. What it does not presently provide is an integrated rule connecting synthetic representation to deceptive authenticity, election-specific disclosure, platform-mediated amplification, and rapid remedial intervention.

The doctrinal result can therefore be stated with greater precision. Of the five SEM elements, the Public Elections Act 2022 already regulates aspects of the electoral nexus, culpability, and democratic harm through offences such as personation, false statements, and undue influence. It does not, however, systematically regulate the synthetic-representation and deceptive-authenticity elements that distinguish SEM from traditional electoral misconduct. Nor does it establish a general provenance obligation through which voters can determine whether apparently authentic political audiovisual material has been artificially generated or materially manipulated. Existing electoral law consequently provides partial substantive coverage but leaves a residual authenticity and enforcement gap.

A comparable but distinct analysis applies to the Cyber Security and Crime Act 2021. Sections 40 and 41 criminalize computer-related forgery and computer fraud, while Section 42 addresses identity theft and impersonation (Cyber Security and Crime Act, 2021). These provisions must likewise be evaluated according to their statutory elements rather than dismissed because they predate widespread generative AI use. A deepfake may fall within their scope where its production or deployment independently satisfies the requirements of computer-related forgery, fraud, identity theft, or impersonation. Yet SEM does not necessarily involve unauthorized system access, fraudulent acquisition of credentials, economic gain or loss, or the forms of identity misuse contemplated by conventional cybercrime provisions. Synthetic content can be generated from lawfully accessible images, recordings, and publicly available data and disseminated through ordinary platform functionality. In such circumstances the legally relevant electoral injury arises from deceptive representation and its effect on democratic choice rather than from intrusion into or manipulation of a protected computer system. Cybercrime law therefore supplies supplementary rather than comprehensive coverage of SEM.

The regulatory position is further shaped by the Independent Media Commission Act 2020. The Act establishes regulatory authority over media institutions through professional standards, media accountability, and responsible journalism. The legal framework should also be read together with the Independent Media Commission (Print and Electronic Media) Regulations 2022, rather than the 2020 Act in isolation (Independent Media Commission Act, 2020). Together, these

instruments provide technology-neutral standards capable of addressing aspects of false or professionally irresponsible content disseminated by actors falling within the Commission's regulatory sphere. Their existence further confirms that synthetic electoral content does not enter an entirely unregulated environment. However, contemporary deepfakes may circulate through global digital platforms, private accounts, encrypted messaging services, influencers, anonymous networks, and algorithmic recommendation systems that do not map neatly onto traditional publisher-based regulatory models. The residual problem is therefore institutional as well as substantive: existing media governance does not establish an election-specific systemic-risk regime requiring major online platforms to assess deepfake risks, preserve provenance information, disclose synthetic political content, cooperate through defined rapid-response procedures, or mitigate algorithmic amplification according to legally specified electoral duties.

This more qualified diagnosis is important for identifying the appropriate comparative inquiry. Foreign legislation is relevant not because Sierra Leone lacks electoral, cybercrime, or media law, but because selected jurisdictions have begun adding legal functions that Sierra Leone's technology-neutral framework does not presently perform. In the United States, the comparative analysis in this study is specifically confined to California, Minnesota, and Washington rather than referring generically to "several states." These jurisdictions were selected because they illustrate three identifiable forms of election-specific synthetic-media regulation. California Elections Code § 20010 regulates materially deceptive audio or visual media of candidates during a defined pre-election period, incorporates a disclosure mechanism, and permits injunctive and civil remedies (Cal. Elec. Code § 20010, 2026). Minnesota Statutes § 609.771 expressly criminalizes specified dissemination of a "deep fake" where the statutory knowledge or recklessness, absence of consent, electoral intent, and temporal requirements are met (Minnesota Legislature, 2025). Washington's RCW § 29B.35.010 defines "synthetic media," permits candidates to seek injunctive and damages remedies for synthetic electioneering communications, recognizes prescribed disclosure as an affirmative defense, and directs expedited judicial treatment (Washington State Legislature, 2025). These provisions differ substantially in design and constitutional implications, but each identifies synthetic representation itself as a legally relevant feature rather than requiring prosecutors or litigants to reconstruct the harm exclusively through conventional personation or false-statement offences (Birrer & Just, 2025).

The comparison is particularly instructive when the elements of those state statutes are placed alongside SEM. California links materially deceptive audiovisual representation to candidate identity, voter deception, intent, temporal proximity to an election, disclosure, and remedies. Minnesota combines realistic technological representation with knowledge or recklessness, non-consent, electoral intent, and a defined electoral period. Washington combines realistic but false synthetic representation with electioneering communication and candidate-focused judicial relief. None provides a universal model for transplantation into Sierra Leone. Their analytical value lies instead in demonstrating that election-specific legislation can define the relationship among synthetic representation, deceptive authenticity, electoral nexus, culpability, protected expression, and remedial urgency with greater precision than a general personation offence.

Recent developments elsewhere reinforce this functional comparison. Article 50(4) of Regulation (EU) 2024/1689 expressly requires disclosure where an AI system generates or manipulates image, audio, or video content constituting a deepfake, subject to qualifications for artistic, creative, satirical, fictional, and analogous works (European Union AI Act, 2024). The Digital Services Act complements this transparency model through Articles 34 and 35, which require very large online platforms and search engines to assess and mitigate defined systemic risks, including risks affecting civic discourse and electoral processes. The EU model therefore contributes primarily transparency and platform-risk governance rather than a single election-specific deepfake criminal offence (Regulation (EU) 2022/2065, 2022).

Singapore provides a different regulatory configuration. Section 61MA of the Parliamentary Elections Act 1954 expressly criminalizes, during an election period, specified online election advertising containing a digitally generated or manipulated audio, visual, or audiovisual representation realistically but falsely depicting a candidate as saying or doing something (Parliamentary Elections Act, 1954). The Act also provides corrective-direction mechanisms in the election-advertising framework. In parallel, the Protection from Online Falsehoods and Manipulation Act 2019 authorizes correction, stop-communication, targeted-correction, and disabling directions and contains specific institutional arrangements for election periods (Protection from Online Falsehoods and Manipulation Act, 2019). Singapore therefore illustrates the combination of an election-specific manipulated-content offence with comparatively rapid administrative response mechanisms.

These comparisons permit a more reproducible assessment than the qualitative labels used in the earlier version of Table 3. Rather than describing jurisdictions simply as “emerging,” “partial,” “strong,” or “fragmented,” the revised comparison evaluates observable legal functions according to four criteria: (1) legal specificity whether primary legislation expressly identifies deepfakes, synthetic media, or digitally manipulated content; (2) electoral specificity whether the rule is directly connected to candidates, campaigns, political advertising, or a defined election period; (3) regulatory reach whether obligations extend beyond content originators to platforms or intermediaries; and (4) remedial capacity whether the framework supplies disclosure, correction, disabling, civil, criminal, injunctive, or expedited remedies. The classifications used in Table 3 are therefore functional legal classifications rather than rankings of regulatory quality. “Explicit” denotes direct statutory recognition of synthetic or manipulated media; “technology-neutral/conditional” denotes potential application only where the elements of a pre-existing general provision are independently satisfied; “jurisdiction-specific” denotes coverage that varies across subnational jurisdictions; and “no dedicated mechanism” denotes the absence of an identified rule specifically performing the regulatory function under examination.

Table 3.
Comparative Functional Coverage of Electoral Deepfake Governance

Regulatory function	Sierra Leone	European Union	Selected United States jurisdictions	Singapore
Express legal recognition of synthetic/deepfake content	Technology-neutral/conditional: PEA 2022 and Cyber Security and Crime Act 2021 may reach specific conduct but do not establish a dedicated SEM category	Explicit: AI Act, Art. 50(4), expressly regulates deepfakes for transparency purposes	Explicit but jurisdiction-specific: California Elections Code § 20010; Minnesota Statutes § 609.771; Washington RCW § 29B.35.010	Explicit and election-specific: Parliamentary Elections Act, § 61MA
Synthetic-content transparency	No dedicated election-specific AI disclosure or provenance duty	Explicit disclosure obligation under AI Act, Art. 50(4)	Jurisdiction-specific: California uses prescribed disclosure; Washington recognizes disclosure as an affirmative defense; Minnesota is primarily	Manipulated-content prohibition and corrective mechanisms operate within the election-advertising framework

Regulatory function	Sierra Leone	European Union	Selected United States jurisdictions	Singapore
Platform/intermediary responsibility	No dedicated election-period systemic-risk regime for major online platforms	Explicit systemic-risk assessment and mitigation duties for VLOPs/VLOSEs under DSA Arts. 34–35	prohibition-oriented Fragmented by state and remedy; no uniform state-law model across the United States	POFMA provides targeted correction, disabling, and other intermediary directions
Election-specific synthetic-media offence or remedy	Technology-neutral/conditional: personation, false statements, undue influence, cybercrime, and media rules may apply depending on their elements	No single election-specific deepfake criminal offence at EU level; transparency and systemic-risk governance provide complementary regulation	Explicit: criminal, civil, disclosure, and injunctive models differ among Minnesota, California, and Washington	Explicit offence under § 61MA for specified manipulated online election advertising
Rapid or expedited response	General electoral and judicial mechanisms exist, but no dedicated synthetic-media emergency procedure	Risk-mitigation and supervisory mechanisms exist, but not a single election-specific emergency deepfake procedure equivalent to the proposed SEIF mechanism	Jurisdiction-specific: California provides priority injunctive relief; Washington encourages expedited determination; Minnesota provides criminal and injunctive mechanisms	Corrective-direction architecture under election law and POFMA permits comparatively rapid intervention

Source: Author's comparative doctrinal analysis of the Public Elections Act 2022 and related Sierra Leonean legislation; Regulation (EU) 2024/1689, Article 50(4); Regulation (EU) 2022/2065, Articles 34–35; California Elections Code § 20010; Minnesota Statutes § 609.771; Washington RCW § 29B.35.010; Singapore Parliamentary Elections Act 1954, § 61MA; and Protection from Online Falsehoods and Manipulation Act 2019.

Table 3 therefore does not establish a hierarchy in which one jurisdiction is categorically “stronger” or more legally developed than another. It identifies which regulatory functions have been juridically specified and through what mechanism. The comparison reveals regulatory specialization rather than institutional superiority. The European Union provides the clearest model of cross-cutting transparency and systemic platform-risk governance; California, Minnesota, and Washington demonstrate alternative state-level approaches to synthetic electoral content through disclosure, criminalization, and civil or injunctive remedies; and Singapore combines an election-specific manipulated-content prohibition with corrective administrative mechanisms. Sierra Leone already possesses technology-neutral rules capable of regulating parts of the same conduct, but those rules remain distributed across electoral, cybercrime, constitutional, and media regimes and are not integrated around synthetic authenticity as a distinct electoral risk.

The significance of the resulting regulatory gap therefore extends beyond legislative omission. The doctrinal finding is not that deepfakes are presently “unregulated” in Sierra Leone. Rather, existing law produces a pattern of partial, offence-specific, and institutionally dispersed coverage. A deepfake may be actionable where it constitutes personation in the statutory sense, falls within

a prohibited false statement, amounts to undue influence, satisfies the elements of a cyber offence, or breaches applicable media standards. Yet materially harmful synthetic electoral content may escape or complicate those categories where the central wrong lies in presenting an artificially constructed political representation as authentic and rapidly amplifying it through digital networks.

This distinction answers the first research question with greater precision. Sierra Leone's existing framework regulates several components of SEM particularly its electoral nexus, culpable interference, and certain manifestations of democratic harm but does not systematically address its synthetic-representation and deceptive-authenticity dimensions, nor the associated requirements of provenance, platform accountability, and time-sensitive electoral response. The resulting problem is therefore one of regulatory incompleteness rather than legal absence. It is this identified residual gap, rather than the mere novelty of AI technology, that provides the doctrinal justification for considering a dedicated Synthetic Electoral Integrity Framework.

3. Towards a Synthetic Electoral Integrity Framework for Sierra Leone

The preceding analysis generated two principal findings. First, deepfakes constitute a distinct category of electoral harm conceptualized in this study as Synthetic Electoral Manipulation (SEM). Second, Sierra Leone's existing constitutional, electoral, cybercrime, and media governance frameworks provide partial and technology-neutral coverage of particular manifestations of SEM but remain fragmented and structurally incomplete in relation to synthetic representation, deceptive authenticity, provenance, platform accountability, and time-sensitive electoral remedies. These findings raise a broader regulatory question: what form of governance architecture is capable of safeguarding electoral integrity within an environment increasingly characterized by AI-generated political communication? Addressing this challenge requires more than isolated legislative amendments. The emergence of synthetic political realities necessitates a comprehensive framework capable of integrating constitutional protections, electoral integrity requirements, technological accountability, and democratic resilience. Accordingly, this article proposes a Synthetic Electoral Integrity Framework (SEIF) as a specialized governance architecture for regulating deepfake-related electoral risks.

Importantly, the five pillars of SEIF are not derived solely from normative theory. Rather, they emerge from a comparative synthesis of the regulatory responses examined in the European Union, the United States, and Singapore (Dziedzic, 2025; Jayakumar et al., 2021; Zheng et al., 2025). More specifically, each pillar is derived through a two-stage analytical process. The first stage identifies a residual regulatory function that Sierra Leone's existing technology-neutral framework does not adequately perform after the applicable constitutional, electoral, cybercrime, and media provisions have been assessed. The second stage examines whether the comparative jurisdictions provide a legally identifiable mechanism capable of performing that function and, if so, extracts the underlying regulatory principle rather than transplanting the foreign rule itself. The resulting pillar is therefore justified only where a demonstrated Sierra Leonean regulatory deficiency corresponds to a comparatively observable governance function that can be constitutionally adapted to the domestic legal order.

This derivation produces five direct relationships. The absence of a legal mechanism for distinguishing harmful synthetic impersonation from protected synthetic expression generates the need for classification. The absence of election-specific provenance and disclosure rules generates the need for transparency obligations. The absence of systemic election-period responsibilities for digital intermediaries generates the need for platform accountability. The incomplete fit between existing personation, false-statement, undue-influence, and cybercrime offences and the constitutive elements of SEM generates the need for narrowly defined electoral deepfake offences. Finally, the absence of a dedicated mechanism capable of responding to high-impact synthetic content within electorally consequential timeframes generates the need for an emergency response procedure. The comparative materials are used to specify how these regulatory functions may be

operationalized while the three theoretical perspectives determine the normative limits within which they may legitimately operate.

Consequently, SEIF should not be understood as an arbitrary collection of regulatory measures. Rather, it represents a synthesized governance model derived from the common regulatory principles observable across the comparative jurisdictions examined in this study. While the European Union contributes primarily to transparency and platform-governance mechanisms (Dziedzic, 2025; Łabuz, 2026), the United States provides important developments in election-specific deepfake regulation (Zheng et al., 2025), and Singapore offers lessons regarding rapid institutional intervention (Jayakumar et al., 2021). Their relevance, however, differs across the five pillars. The European Union principally informs the transparency and systemic-risk functions; the selected United States jurisdictions demonstrate how synthetic electoral representations may be subjected to election-specific disclosure, civil, injunctive, or criminal rules; and Singapore demonstrates how manipulated electoral content may be combined with comparatively rapid corrective intervention. These functions are then filtered through Sierra Leone's constitutional guarantees of political expression, electoral participation, due process, and institutional accountability. The resulting framework adapts these principles to the institutional realities of Sierra Leone and similarly situated emerging democracies while remaining grounded in Electoral Integrity Theory, Information Disorder Theory, and Digital Constitutionalism (De Gregorio, 2022; Norris, 2014; Wardle & Derakhshan, 2017). **Table 4** makes this derivation explicit by linking each pillar to four components: the Sierra Leonean doctrinal finding that generates the regulatory problem, the comparative mechanism from which a transferable governance function is identified, the theoretical principle governing its legitimate use, and the resulting SEIF pillar.

Table 4.
Doctrinal, Comparative, and Theoretical Derivation of the Synthetic Electoral Integrity Framework (SEIF)

Sierra Leonean doctrinal finding	Comparative governance function	Theoretical basis	Resulting SEIF pillar
Existing personation, false-statement, cybercrime, and media rules may reach particular conduct but do not provide a general legal distinction between harmful synthetic electoral deception and protected satire, parody, journalism, or transparently artificial political expression.	Comparative approaches demonstrate the use of defined synthetic-media categories, material-deception thresholds, disclosure rules, and expressive exceptions to delimit regulatory scope.	Digital Constitutionalism: legal certainty, proportionality, freedom of expression, and limits on state discretion.	Electoral Deepfake Classification System
Existing law contains no dedicated election-specific provenance or AI-content disclosure obligation enabling voters systematically to identify materially synthetic political audiovisual content.	The European Union's transparency-oriented AI governance and disclosure-based approaches identified in comparative electoral regulation demonstrate mechanisms for revealing the artificial origin of synthetic content without necessarily prohibiting it.	Information Disorder Theory + Digital Constitutionalism: authentication, voter autonomy, transparency, and proportionate intervention.	Political AI Transparency Obligations
Sierra Leone lacks a dedicated election-period systemic-risk framework governing algorithmic amplification, platform risk assessment, synthetic-content mitigation, and structured	The European Union's Digital Services Act illustrates systemic-risk assessment, mitigation, transparency, and intermediary-accountability	Information Disorder Theory: amplification dynamics and systemic dissemination of deceptive content.	Platform Accountability Duties

Sierra Leonean doctrinal finding	Comparative governance function	Theoretical basis	Resulting SEIF pillar
cooperation between major platforms and electoral authorities.	functions applicable to large digital platforms.		
Technology-neutral offences such as personation, false statements, undue influence, forgery, fraud, and identity-related provisions provide conditional coverage but do not systematically integrate synthetic representation, deceptive authenticity, electoral nexus, culpability, and democratic harm within a single election-specific legal category.	Selected United States jurisdictions and Singapore demonstrate election-specific legal treatment of materially deceptive or digitally manipulated candidate representations through criminal, civil, disclosure, and injunctive mechanisms.	Electoral Integrity Theory + Digital Constitutionalism: protection of fair competition subject to legality, culpability, necessity, and proportionality.	Electoral Deepfake Offences
General judicial, electoral, cybercrime, and media procedures provide no dedicated mechanism specifically designed to address electorally consequential synthetic content whose democratic effects may become irreversible before ordinary proceedings conclude.	Singapore's corrective mechanisms and expedited approaches identified in comparative electoral regulation demonstrate the regulatory function of time-sensitive intervention subject to legally defined safeguards.	Electoral Integrity Theory + Digital Constitutionalism: effective electoral protection constrained by due process, temporality, proportionality, and review.	Emergency Electoral Response Mechanism

Source: Author's synthesis of the doctrinal findings concerning Sierra Leone's Constitution, Public Elections Act 2022, Cyber Security and Crime Act 2021, Independent Media Commission Act 2020 and related media regulation, together with the comparative analysis of European Union, selected United States, and Singaporean regulatory approaches and the analytical perspectives of Electoral Integrity Theory, Information Disorder Theory, and Digital Constitutionalism.

The first pillar of SEIF is the Electoral Deepfake Classification System. Effective regulation requires legal differentiation between categories of synthetic content because not all AI-generated political communication poses equivalent risks to democratic processes. This pillar responds directly to the doctrinal finding that Sierra Leone's existing technology-neutral offences regulate specific forms of personation, false statements, undue influence, and related misconduct but do not provide a general legal test for determining when synthetic political representation becomes SEM. Without such a threshold, regulatory intervention risks either under-inclusion, where harmful synthetic impersonation escapes existing categories, or over-inclusion, where legitimate satire, parody, journalism, artistic expression, or transparently synthetic political communication is unnecessarily restricted. Consequently, the framework distinguishes between deceptive deepfakes intended to mislead voters, manipulative deepfakes designed to influence electoral behavior through fabricated representations, and protected forms of satire, parody, artistic expression, or political commentary.

Comparatively, this classification function is supported by regulatory approaches that distinguish materially deceptive or realistically false synthetic representations from protected or adequately disclosed content. The transferable principle is not the wholesale adoption of any foreign definition, but the requirement that legal intervention be triggered by identifiable criteria concerning synthetic representation, deceptive authenticity, electoral nexus, culpability, and democratic harm. This approach reflects the influence of Digital Constitutionalism and draws inspiration from the European Union's emphasis on legal certainty, proportionality, and rights-based governance (De Gregorio, 2022; Łabuz, 2026). By distinguishing harmful synthetic manipulation from legitimate expressive activity, the framework seeks to balance electoral protection with constitutional guarantees of freedom of expression.

The second pillar consists of Political AI Transparency Obligations. Information Disorder Theory suggests that democratic harm frequently arises when citizens are unable to distinguish authentic political communication from manipulated content (Vaccari & Chadwick, 2020; Wardle & Derakhshan, 2017). The doctrinal basis for this pillar is the identified absence in Sierra Leone's electoral, cybercrime, and media framework of a dedicated election-specific obligation requiring political actors systematically to disclose the materially artificial origin of synthetic campaign content. Existing false-statement or media provisions may regulate the substantive content of particular communications, but they do not perform the separate regulatory function of provenance: enabling the electorate to determine whether apparently authentic audiovisual evidence has been artificially generated or materially manipulated.

Accordingly, political actors utilizing AI-generated electoral content should be subject to mandatory disclosure requirements. Such obligations may include visible content labelling, digital watermarking, provenance verification systems, and public disclosure of AI-assisted campaign materials. The comparative analysis supplies the functional model for this response. Transparency-oriented AI regulation demonstrates that synthetic content can be governed through disclosure rather than prohibition, while comparative election-specific rules show that appropriate labelling can differentiate lawful synthetic political expression from covert deception. SEIF therefore translates the comparative principle of provenance transparency into an electoral obligation responsive to Sierra Leone's identified disclosure gap. This pillar reflects emerging transparency-oriented approaches observed within comparative regulatory systems (Łabuz, 2026; Steinebach et al., 2026). Transparency obligations therefore do not prohibit synthetic content but instead enhance voter autonomy by enabling citizens to evaluate political communication with knowledge of its artificial origins.

The third pillar establishes Platform Accountability Duties. Contemporary electoral communication increasingly occurs through digital platforms whose recommendation algorithms influence the visibility, amplification, and dissemination of political content (Helberger, 2020; Shaholli, 2025). Deepfakes therefore present not only a content problem but also a platform-governance challenge. This pillar follows directly from the institutional gap identified in the preceding doctrinal analysis: Sierra Leone possesses electoral, cybercrime, and media rules applicable to particular speakers or forms of misconduct, but it lacks an election-specific systemic-risk regime imposing defined responsibilities upon major digital intermediaries for algorithmic amplification, provenance preservation, risk assessment, and cooperation during electoral periods. The problem is therefore not simply that harmful content appears online; it is that platform architecture can transform an individual act of synthetic deception into a systemic electoral risk.

Drawing upon Information Disorder Theory and informed by regulatory developments within the European Union, particularly platform-risk governance approaches, SEIF imposes election-period obligations upon platforms such as Meta, TikTok, YouTube, and X (De Gregorio, 2022; Dziedzic, 2025). The comparative derivation is especially direct here. The Digital Services Act demonstrates a governance model in which large intermediaries are required to identify and mitigate systemic risks rather than merely remove individually unlawful items after harm has occurred. SEIF extracts that systemic-responsibility function and adapts it to the narrower electoral context identified by the Sierra Leonean analysis. These obligations include risk assessments, transparency reporting, synthetic-content detection mechanisms, cooperation with electoral authorities, and procedures for mitigating the rapid dissemination of harmful electoral deepfakes. The objective is not to transform platforms into arbiters of truth but to require reasonable measures for reducing systemic democratic risks.

The fourth pillar introduces Electoral Deepfake Offences. Electoral Integrity Theory maintains that democratic competition requires protection against conduct capable of distorting electoral outcomes (Norris, 2014). The doctrinal justification for this pillar is not the absence of existing electoral offences. As demonstrated in the preceding section, provisions governing

personation, false statements, undue influence, cyber-enabled impersonation, and related misconduct may already apply to particular deepfake scenarios where their statutory elements are satisfied. The residual deficiency is that these provisions regulate discrete manifestations of misconduct but do not systematically capture the conjunction of synthetic representation, deceptive authenticity, electoral nexus, legally relevant culpability, and democratic harm that defines SEM. The proposed offence therefore supplements rather than displaces technology-neutral electoral law.

Existing electoral offences should therefore be expanded or supplemented through narrowly defined provisions encompassing candidate impersonation, fabricated endorsements, voter-suppression deepfakes, synthetic campaign fraud, and comparable AI-generated electoral deception. Comparative analysis of election-specific synthetic-media regulation in selected United States jurisdictions and Singapore demonstrates that legislatures can define manipulated candidate representations as a distinct electoral regulatory object while differentiating criminal, civil, injunctive, and disclosure-based consequences. The transferable principle is legal specificity: liability should attach not because AI has been used, but because the prescribed elements of deceptive synthetic electoral interference are satisfied. This pillar therefore draws support from developments in jurisdictions where election-specific measures recognize AI-generated political impersonation as a distinct threat to electoral integrity (Soñeca, 2025; Zheng et al., 2025).

Consistent with the SEM definition developed in this study, punitive liability should require clear proof of the prohibited synthetic representation, its electoral nexus, deceptive presentation, the requisite mental element, and the legally specified harm or material risk of harm. Criminalization is justified where synthetic content is deliberately deployed to undermine electoral fairness, interfere with democratic participation, or manipulate voter decision-making. The objective is not to criminalize technological innovation but to deter conduct that threatens the integrity of electoral competition.

The fifth pillar establishes an Emergency Electoral Response Mechanism. Deepfakes possess the capacity to spread rapidly and generate electoral effects within hours rather than weeks (Chesney & Citron, 2019; Diakopoulos & Johnson, 2021). Conventional judicial procedures may therefore prove inadequate during election periods. This pillar is derived from the remedial gap identified in Sierra Leone's existing framework. Even where a technology-neutral electoral, cybercrime, or media provision ultimately applies, legal entitlement without timely remedial capacity may provide little effective protection where a fabricated candidate withdrawal, false voting instruction, synthetic institutional announcement, or similar manipulation circulates immediately before polling. The relevant regulatory deficiency is thus temporal: the ordinary availability of ex post liability does not necessarily prevent an electorally irreversible harm.

To address this challenge, SEIF authorizes expedited review procedures, rapid takedown mechanisms, emergency fact-verification processes, and temporary intervention powers for electoral authorities subject to subsequent judicial oversight. Comparatively, Singapore's corrective regulatory architecture illustrates the governance function of rapid intervention against harmful digital content, while other election-specific approaches examined in the comparative analysis demonstrate the importance of expedited injunctive remedies. SEIF derives from these models not a general administrative power to determine political truth, but a narrowly delimited capacity to respond to demonstrably synthetic electoral interference before the relevant electoral harm becomes irreversible.

This pillar reflects the combined influence of Electoral Integrity Theory and Digital Constitutionalism while drawing comparative inspiration from Singapore's emphasis on rapid institutional response to harmful digital content (De Gregorio, 2022; Jayakumar et al., 2021). Importantly, emergency powers must remain subject to proportionality requirements, due-process guarantees, and judicial accountability to prevent misuse for political purposes. Their exercise should therefore be conditioned upon a defined electoral period, prima facie evidence that the

content satisfies the SEM criteria, necessity of intervention to avert material electoral harm, the availability of reasoned decisions, temporal limitation of any interim measure, and prompt access to independent judicial review. In this manner, the remedial mechanism answers the identified enforcement gap without converting electoral authorities into unconstrained regulators of political discourse.

Collectively, these five pillars constitute the Synthetic Electoral Integrity Framework. Their relationship is cumulative rather than merely additive. Classification determines whether synthetic content falls within the regulatory domain; transparency reduces deception before coercive intervention becomes necessary; platform duties address systemic dissemination; specialized offences allocate liability where culpable synthetic interference satisfies defined legal elements; and emergency procedures provide temporally effective remedies where delay would defeat electoral protection. Each pillar therefore addresses a distinct deficiency identified through the doctrinal analysis, while each corresponding regulatory function is informed by but not transplanted from the comparative jurisdictions.

The framework advances beyond traditional election law by recognizing Synthetic Electoral Manipulation as a distinct legal category and by constructing a governance architecture specifically tailored to the realities of algorithmically mediated political communication. Its principal contribution lies not merely in proposing legal reform but in establishing a theory-informed and comparatively grounded model for regulating the production, dissemination, and governance of synthetic political realities. By integrating the normative commitments of Electoral Integrity Theory, Information Disorder Theory, and Digital Constitutionalism with regulatory lessons drawn from the European Union, the United States, and Singapore (De Gregorio, 2022; Norris, 2014; Wardle & Derakhshan, 2017; Zheng et al., 2025), SEIF provides a coherent legal architecture capable of protecting electoral integrity while preserving democratic participation and freedom of expression in the age of generative artificial intelligence.

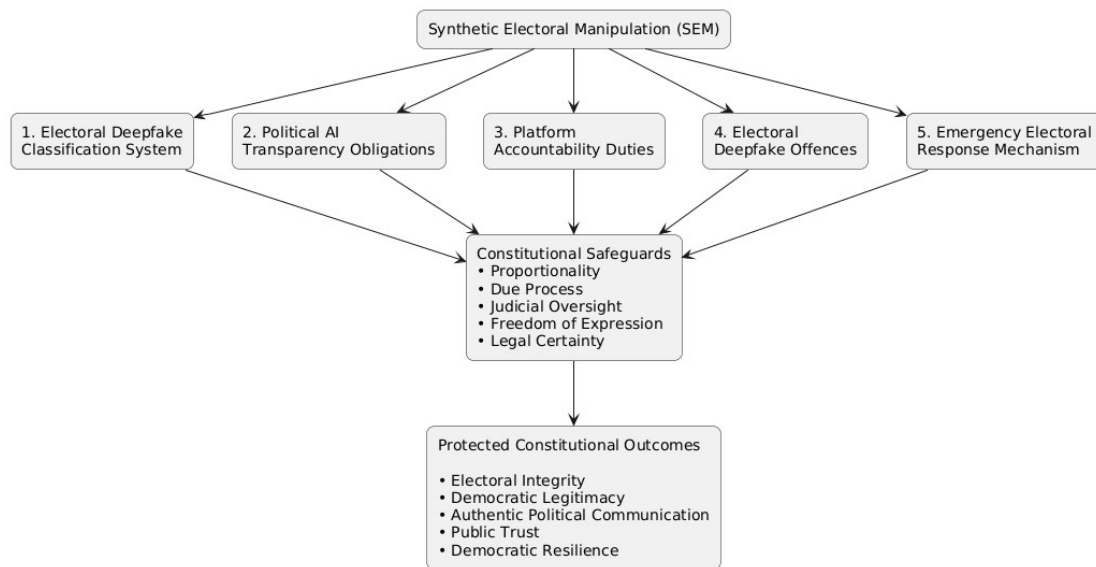


Figure 2. Synthetic Electoral Integrity Framework (SEIF): Governance Architecture

Source: Author's synthesis based on Electoral Integrity Theory, Information Disorder Theory, Digital Constitutionalism, the doctrinal analysis of Sierra Leone's existing legal framework, and comparative regulatory analysis of the European Union, selected United States jurisdictions, and Singapore.

Figure 2 presents the governance architecture proposed in this study. Rather than treating electoral deepfakes as isolated legal problems, SEIF integrates five complementary governance functions that collectively address the lifecycle of Synthetic Electoral Manipulation (SEM), from

identification and transparency to institutional accountability, legal enforcement, and emergency electoral protection. The figure should therefore be read as the visual synthesis of the preceding derivation: each component corresponds to a regulatory deficiency established doctrinally and a governance function identified comparatively, while the framework as a whole remains bounded by constitutional requirements of legality, proportionality, due process, and freedom of expression.

4. Constitutional Legitimacy and Safeguards in Regulating Synthetic Electoral Manipulation

The recognition of Synthetic Electoral Manipulation (SEM) as a distinct category of electoral harm raises a constitutional question extending beyond electoral administration itself: under what conditions may democratic states regulate AI-generated political communication without undermining the constitutional freedoms that elections are intended to protect? While the preceding sections establish the regulatory necessity of addressing deepfake-enabled electoral manipulation, constitutional legitimacy cannot be derived solely from the existence of a regulatory gap. In Sierra Leone, that legitimacy must be determined primarily by reference to the Constitution of Sierra Leone 1991 rather than by an externally derived theory of digital governance. Section 25 protects freedom of expression, including the freedom to hold opinions and to receive and impart ideas and information, while simultaneously permitting legally prescribed restrictions where they are reasonably required for constitutionally recognized purposes and remain reasonably justifiable in a democratic society. Section 31 guarantees eligible citizens the right to vote; Sections 32 and 33 establish the Electoral Commission and entrust it with constitutionally protected responsibility for the conduct and supervision of public elections and referenda; and Section 36 reinforces the constitutional architecture of electoral choice through secret voting (Constitution of Sierra Leone, 1991). Read together, these provisions create the domestic constitutional parameters within which SEM regulation must operate: political expression is presumptively protected, electoral participation must remain meaningful, electoral administration must remain institutionally independent, and restrictions upon political communication require democratic justification. The constitutional challenge therefore lies not in choosing between electoral integrity and fundamental rights, but in designing a governance framework capable of protecting both simultaneously (Green et al., 2025). Effective regulation consequently requires a structured constitutional balancing exercise rather than an unrestricted expansion of governmental regulatory authority (Cárdenas Gracia, 2014).

Digital Constitutionalism performs a supporting rather than constitutive role in this analysis. The legal authority for regulating SEM derives from Sierra Leone's constitutional text; Digital Constitutionalism assists in interpreting how established constitutional commitments should operate when political communication is mediated by algorithmic systems and synthetic media. In particular, its emphasis on legal certainty, transparency, institutional accountability, rights protection, and constraints on technologically enabled public and private power provides an analytical vocabulary through which the implications of Sections 25 and 31–36 may be assessed in the digital electoral environment (De Gregorio, 2022). It does not create additional constitutional rights or displace the limitations framework contained in Section 25. Within digitally mediated public spheres, constitutional obligations extend beyond protecting individuals from governmental interference to safeguarding the institutional conditions necessary for meaningful democratic participation (Basanta Vázquez & Azurmendi, 2025; Kučs, 2025; Rocha, 2026). The relevant constitutional proposition is therefore narrower than asserting a general state obligation to guarantee informational truth. Sierra Leone's Constitution protects political communication and voting while constitutionally organizing the institutions through which electoral choice is exercised. Where deliberately deceptive synthetic representations materially interfere with those protected processes, regulation may pursue a constitutionally legitimate electoral objective, but only within the limits imposed by the Constitution itself.

This perspective reflects an important evolution in constitutional understandings of electoral rights. Traditionally, constitutional protection has concentrated upon safeguarding the right to vote, political equality, freedom of political expression, and procedural fairness during electoral processes (Chrysogonos & Stratilatis, 2012). Generative artificial intelligence fundamentally alters this constitutional landscape by threatening the informational environment within which these rights are exercised (Ferrara, 2025; Lin, 2025). Deepfakes capable of fabricating candidate statements, manipulating campaign events, or creating fictitious political endorsements interfere not merely with individual speech but with the authenticity of democratic deliberation itself (Kopecky, 2024). The constitutional implication, however, should not be overstated. Neither Section 25 nor Sections 31–36 expressly recognize a freestanding right to “electoral authenticity,” nor does this study claim that such an autonomous constitutional right presently exists in Sierra Leonean law. Rather, this article advances a normative and doctrinal argument that electoral authenticity may be understood as a derivative constitutional interest arising from the interaction of existing constitutional guarantees.

The argument proceeds in three steps. First, Section 31 protects the citizen's right to vote, but the meaningful exercise of that right occurs within an electoral process constitutionally administered and supervised under Sections 32 and 33. Second, Section 25 protects the communicative environment in which political information, opinions, and electoral advocacy circulate, while its limitation clause recognizes that expression may in defined circumstances be regulated to protect competing rights and public interests, provided the interference is reasonably required and reasonably justifiable in a democratic society. Third, synthetic representations that deliberately fabricate apparently authentic candidate speech, electoral instructions, institutional announcements, or other electorally consequential events may impair the effective exercise of these existing constitutional interests without necessarily falling within conventional categories of physical coercion or personation. On this basis, “electoral authenticity” is used in this study not as an independent constitutional entitlement to truthful politics, but as a derivative interest in preserving the minimum conditions of communicative authenticity necessary for the meaningful exercise of constitutionally protected electoral participation.

This derivative formulation is deliberately limited. Democratic politics necessarily accommodates inaccurate claims, partisan rhetoric, exaggeration, satire, parody, contested interpretations, and protected political criticism. The Constitution cannot plausibly be interpreted as guaranteeing citizens an error-free political information environment. The legally relevant threshold arises instead where synthetic content satisfies the constitutive elements of SEM identified in this study: an artificial or materially manipulated representation, a demonstrable electoral nexus, deceptive presentation as authentic, legally relevant culpability, and actual or materially foreseeable harm to protected electoral interests. Electoral authenticity therefore functions as a justificatory constitutional interest only at the intersection between deceptive synthetic representation and the effective exercise of existing constitutional rights and institutions.

Recognizing this derivative interest in electoral authenticity, however, does not justify unrestricted governmental regulation of synthetic political content (Rubio Núñez, 2025). An equally significant constitutional risk arises where broadly drafted regulatory powers enable political authorities to suppress legitimate criticism, opposition speech, investigative journalism, satire, or political dissent under the pretext of combating deepfakes (Balendra, 2024; Zafarullah & Nughat, 2026). This concern is particularly acute within emerging democracies where institutional independence may remain vulnerable to political influence and emergency powers have historically been susceptible to executive expansion (Dressel, 2012; Mbithi & Kijima, 2026). Accordingly, any governance framework that prioritizes electoral protection while neglecting constitutional safeguards risks replacing one democratic threat with another. Section 25 supplies the central domestic constitutional discipline here: a restriction upon synthetic political communication cannot be justified merely by characterizing the content as technologically novel

or socially undesirable. It must have a lawful constitutional purpose, be reasonably required in relation to that purpose, and remain reasonably justifiable in a democratic society. Constitutional legitimacy therefore depends not only upon preventing AI-enabled electoral manipulation but equally upon constraining governmental discretion through objective legal standards, procedural safeguards, and independent institutional oversight.

Potential objections to election-specific deepfake regulation reinforce the importance of these constitutional constraints. Critics may argue that legal regulation of synthetic political communication risks encouraging over-censorship, excessive platform moderation, innovation chilling effects, or politically motivated restrictions on electoral discourse (Cea et al., 2025; Labuz, 2026). Others may contend that rapidly evolving AI technologies make statutory definitions obsolete or create unacceptable risks of false identification and over-enforcement. These concerns are constitutionally significant and cannot be dismissed as merely implementation challenges (Greenstein & Zamboni, 2025; Hammouri, 2024). Instead, they demonstrate that effective regulation must incorporate safeguards that minimize regulatory overreach while maintaining democratic resilience. Within Sierra Leone's constitutional framework, these concerns can be translated into a structured legitimacy inquiry. A SEM-related restriction should therefore satisfy at least five conditions: it must (1) have a clear basis in law; (2) pursue a constitutionally legitimate electoral objective linked to the protection of voting, electoral administration, or the rights and freedoms of others; (3) target conduct falling within sufficiently precise SEM criteria rather than political falsity generally; (4) impose no greater restriction upon expression than is reasonably required to address the demonstrated electoral risk; and (5) remain subject to procedurally independent review and effective legal challenge. These conditions operationalize the constitutional requirements derived principally from Sections 25 and 31–33, while Digital Constitutionalism supports their application to technologically mediated electoral governance. The constitutional legitimacy of regulating SEM therefore depends not upon maximizing state intervention but upon ensuring that regulatory authority remains narrowly tailored, proportionate, evidence-based, and subject to meaningful legal accountability.

For this reason, the proposed Synthetic Electoral Integrity Framework (SEIF) incorporates multiple constitutional safeguards intended to reconcile democratic protection with individual rights. First, the Electoral Deepfake Classification System distinguishes manipulative synthetic political content from satire, parody, artistic expression, journalistic investigation, research, and other constitutionally protected forms of communication. Regulatory intervention is therefore directed exclusively toward deceptive electoral manipulation rather than political opinion or legitimate democratic criticism. This classification function responds directly to Section 25 by narrowing the regulatory object according to the legally relevant characteristics of SEM rather than the viewpoint, political message, or ideological content of the communication. Second, Political AI Transparency Obligations prioritize disclosure over prohibition by requiring political actors to identify AI-generated electoral content through visible labeling, provenance mechanisms, and disclosure obligations. Rather than restricting political expression, these measures strengthen voter autonomy by enabling citizens to evaluate political communication with knowledge of its synthetic origin. Because disclosure ordinarily interferes less directly with political communication than categorical suppression, it also provides a constitutionally preferable first-line response where transparency is sufficient to address the relevant deception. Third, Platform Accountability Duties impose procedural responsibilities including risk assessment, transparency reporting, cooperation with electoral authorities, and mitigation of systemic electoral risks without requiring private digital platforms to become arbiters of political truth. This procedural approach reduces the likelihood of arbitrary content moderation while strengthening institutional responsibility for protecting democratic processes.

Constitutional safeguards assume particular importance during election periods when deepfakes possess the capacity to influence electoral outcomes within extremely short timeframes.

Although delayed judicial proceedings may be insufficient to prevent irreparable democratic harm, expedited intervention cannot displace constitutional guarantees of due process (Curran, 2022; Rouméas, 2022). Emergency Electoral Response Mechanisms should therefore operate only during clearly defined electoral periods, apply exclusively where demonstrable and evidence-based risks to electoral integrity exist, and remain subject to prompt judicial review. The institutional design must also respect the constitutional position of the Electoral Commission under Sections 32 and 33. Because the Constitution establishes the Commission as the body responsible for conducting and supervising elections and protects the exercise of its constitutional functions from external direction or control, any SEIF emergency competence allocated to the Commission should reinforce rather than compromise that institutional independence. Equally, Commission action affecting protected political expression must remain legally bounded and reviewable; constitutional independence cannot be converted into immunity from legality, procedural fairness, or judicial supervision. Independent oversight by the Electoral Commission, the judiciary, and other constitutionally established institutions further limits opportunities for partisan misuse of emergency powers. By embedding proportionality, necessity, temporal limitation, judicial supervision, and procedural accountability within emergency intervention, SEIF seeks to ensure that exceptional regulatory authority remains constitutionally constrained even under urgent electoral conditions.

The comparative analysis undertaken in this study serves a corroborative rather than foundational constitutional function. Although the European Union, the United States, and Singapore adopt distinct constitutional traditions and regulatory philosophies, each increasingly recognizes that AI-generated electoral manipulation requires legal adaptation while simultaneously preserving fundamental constitutional guarantees (Cupać & Sienknecht, 2024; Stavridou, 2025; Tan & Grofman, 2018; Vujicic, 2025). The European Union emphasizes proportionality, transparency, legal certainty, and fundamental rights through its evolving AI governance framework (Cupać & Sienknecht, 2024). Election-specific legislation adopted in the selected United States jurisdictions examined in this study reflects continuing efforts to reconcile electoral protection with constitutional commitments to freedom of expression (Vujicic, 2025). Singapore demonstrates the importance of rapid institutional response while simultaneously relying upon legally prescribed administrative procedures and institutional accountability (Tan & Grofman, 2018). These approaches do not determine the constitutional validity of SEIF in Sierra Leone; that question must ultimately be resolved under the Sierra Leonean Constitution. Their comparative significance lies in demonstrating alternative institutional techniques through which transparency, precision, procedural safeguards, and timely electoral remedies can be incorporated into synthetic-media regulation. Despite significant institutional differences, these regulatory models therefore provide comparative support for, rather than the legal source of, the principle that intervention against synthetic political communication must remain constrained by objective legal standards, procedural fairness, judicial oversight, and institutional accountability (Baltezarević et al., 2025; Romanishyn et al., 2025).

Accordingly, the constitutional legitimacy of regulating Synthetic Electoral Manipulation derives not from expanding governmental control over political communication but from preserving the constitutional conditions necessary for democratic self-government. Under the Sierra Leonean Constitution, the central tension is internal to the constitutional order itself: Section 25 protects political expression while Sections 31–36 establish and protect the institutions and processes through which electoral choice is exercised. The regulatory task is therefore to preserve the effective enjoyment of both sets of constitutional commitments rather than subordinating one to the other. Democratic elections cannot remain genuinely free where citizens are systematically exposed to algorithmically fabricated political realities capable of distorting informed political judgment, nor can they remain constitutionally legitimate where regulatory responses become instruments of censorship or political abuse.

The concept of electoral authenticity advanced here should accordingly be understood as a derivative constitutional justification for carefully delimited intervention, not as a newly discovered textual right. Its legal force depends upon demonstrating, in a particular regulatory context, that deceptive synthetic representation materially threatens the exercise of rights or institutional interests already protected by the Constitution and that the proposed response satisfies the constitutional requirements governing restrictions on expression. Constitutional resilience therefore depends upon maintaining an equilibrium in which freedom of expression, electoral integrity, democratic accountability, technological innovation, and the rule of law operate as mutually reinforcing constitutional commitments rather than competing constitutional values. By embedding the Section 25 democratic-justification standard, clear statutory definition, necessity, proportionality, procedural accountability, Electoral Commission independence, and judicial review within its institutional design, the Synthetic Electoral Integrity Framework advances a constitutionally legitimate governance model capable of protecting electoral integrity while preserving the democratic freedoms upon which constitutional government ultimately depends.

5. Theoretical Contributions and Implications for Emerging Democracies

Beyond its immediate relevance to Sierra Leone, this study advances broader debates in electoral law, artificial intelligence governance, constitutional theory, and comparative public law by demonstrating that generative artificial intelligence challenges not merely the effectiveness of existing legal rules but the conceptual foundations upon which contemporary electoral regulation has been constructed. Existing scholarship has largely examined deepfakes through the analytical frameworks of misinformation, platform governance, cyber regulation, or AI ethics, thereby treating synthetic political content as a technological extension of established legal categories (Chesney & Citron, 2019; Diakopoulos & Johnson, 2021; Floridi et al., 2018; Helberger, 2020). This study advances a different theoretical position. It argues that AI-generated electoral manipulation constitutes a qualitatively distinct form of democratic harm because its primary mechanism is not the dissemination of false information but the algorithmic construction of synthetic political realities capable of altering citizens' perceptions of authenticity itself. Consequently, the appropriate regulatory object is no longer informational falsity alone but the constitutional protection of authentic democratic deliberation.

The first theoretical contribution therefore lies in the conceptualization of Synthetic Electoral Manipulation (SEM) as a distinct legal category of electoral interference. SEM is not introduced as a terminological refinement of misinformation or disinformation, but as a reconceptualization of electoral harm that identifies synthetic authenticity as the legally significant object of regulation. Whereas conventional legal frameworks regulate deceptive statements, fraudulent conduct, or unlawful electoral influence, SEM explains how generative artificial intelligence enables democratic manipulation through the creation of fabricated yet apparently authentic political realities (Ferrara, 2025; Vaccari & Chadwick, 2020; Wardle & Derakhshan, 2017). This conceptual shift extends existing scholarship by demonstrating that algorithmically generated authenticity can acquire derivative constitutional significance where synthetic deception materially impairs constitutionally protected electoral rights or institutions. Accordingly, the study reframes electoral harm from a problem of informational falsity to one concerning the epistemic conditions necessary for meaningful democratic participation and electoral integrity.

The second contribution extends Electoral Integrity Theory. Conventional understandings of electoral integrity have emphasized procedural fairness, equal political competition, transparency, and effective electoral administration (Norris, 2014; van Ham, 2020). These principles remain indispensable but were developed within an informational environment in which the authenticity of political communication was largely presumed rather than contested (Norris, 2014). Generative artificial intelligence fundamentally alters this assumption. Electoral integrity must now encompass protection against synthetic manipulation capable of undermining the informational

conditions necessary for meaningful democratic participation. This study therefore argues that informational authenticity should be recognized as an additional dimension of contemporary electoral integrity because democratic participation depends not only upon free voting procedures but also upon citizens' ability to distinguish genuine political communication from algorithmically fabricated representations. The article consequently expands Electoral Integrity Theory beyond procedural administration toward protection of the epistemic conditions sustaining democratic legitimacy.

A third contribution concerns Digital Constitutionalism. Existing constitutional scholarship frequently frames AI governance as a balance between freedom of expression and governmental regulation (Balendra, 2024; De Gregorio, 2022; Pollicino & Romeo, 2016). While this remains an important constitutional question, the present study demonstrates that AI-generated political communication challenges constitutional democracy at a deeper institutional level. Deepfakes undermine public confidence in the authenticity of democratic communication itself, thereby weakening the informational infrastructure upon which constitutional self-government depends. Constitutional adaptation therefore requires more than recalibrating competing rights. It requires recognizing that constitutional legitimacy increasingly depends upon preserving trustworthy digital public spheres capable of supporting informed democratic deliberation. Within this framework, constitutional protection extends beyond safeguarding individual liberties to maintaining the institutional conditions necessary for authentic democratic participation in digitally mediated societies.

The fourth contribution is methodological and comparative. Rather than treating comparative law as an exercise in institutional borrowing, the study employs comparative legal analysis to identify transferable governance functions operating across different constitutional traditions. The European Union, the United States, and Singapore were not selected as models for legal transplantation but as analytically distinct regulatory systems that collectively illustrate alternative approaches to balancing democratic protection, technological innovation, and constitutional rights (Cupać & Sienknecht, 2024; Jayakumar et al., 2021; Zheng et al., 2025). This functional comparative approach demonstrates that regulatory effectiveness depends less upon replicating foreign institutions than upon adapting common governance principles including transparency, accountability, proportionality, legal certainty, and institutional responsiveness to domestic constitutional contexts. The study therefore contributes to comparative legal methodology by illustrating how governance principles may be transferred without assuming institutional convergence.

These theoretical developments provide the foundation for the article's principal normative contribution: the Synthetic Electoral Integrity Framework (SEIF). Unlike many regulatory proposals that consist primarily of legislative recommendations, SEIF is constructed as a theory-informed governance architecture derived from doctrinal analysis, comparative legal evaluation, and constitutional theory. Its five integrated pillars the Electoral Deepfake Classification System, Political AI Transparency Obligations, Platform Accountability Duties, Electoral Deepfake Offences, and the Emergency Electoral Response Mechanism translate abstract constitutional principles into a coherent regulatory model capable of addressing the institutional realities of AI-mediated electoral communication. Consequently, SEIF should be understood not merely as a policy proposal for Sierra Leone but as a conceptual governance framework explaining how constitutional democracies may regulate synthetic political communication while preserving fundamental rights.

The study also contributes to emerging debates concerning democratic resilience in the age of artificial intelligence. Existing scholarship frequently conceptualizes democratic resilience in terms of institutional continuity, electoral administration, or resistance to political instability (Norris, 2014; Romanishyn et al., 2025). The analysis developed here suggests that resilience must additionally encompass the capacity of constitutional systems to withstand synthetic informational

threats capable of systematically eroding public confidence in democratic institutions. Electoral resilience therefore depends not only upon institutional durability but also upon preserving the authenticity of democratic communication before electoral legitimacy is irreversibly compromised. By theorizing epistemic integrity as an important condition for democratic resilience, the study broadens existing understandings of how constitutional systems should respond to technologically mediated threats.

The implications of these findings extend well beyond Sierra Leone. Across Africa, Asia, Latin America, and other emerging democratic contexts, electoral institutions increasingly operate within digitally mediated communication environments while relying upon constitutional and electoral frameworks originally designed for analogue political processes (Goswami & Sachdeva, 2025; Sam, 2019). Although institutional capacities differ considerably across jurisdictions, the regulatory challenges identified in this study reflect broader structural tensions confronting constitutional democracies adapting to generative artificial intelligence (Ferrara, 2025; Núñez Rocha, 2025). The conceptual framework developed here therefore provides an analytical foundation for future comparative research by demonstrating that effective AI governance requires the integration of constitutional law, electoral regulation, digital governance, and platform accountability within a coherent legal architecture rather than through fragmented legislative intervention.

Finally, the study contributes to the broader field of AI governance by demonstrating that sustainable regulation should be grounded in enduring constitutional principles rather than technology-specific legislative responses alone. Because generative artificial intelligence will continue to evolve beyond existing statutory definitions, durable governance cannot depend exclusively upon regulating particular technological applications (Greenstein & Zamboni, 2025; Zheng et al., 2025). Instead, regulatory legitimacy should derive from constitutional principles capable of adapting to future technological developments while preserving democratic participation, proportionality, transparency, accountability, legal certainty, and the rule of law. By integrating these constitutional commitments within a coherent governance architecture, the Synthetic Electoral Integrity Framework advances a theoretically grounded model for strengthening democratic resilience while preserving fundamental rights in the age of artificial intelligence. Collectively, these contributions position the present study not simply as an examination of electoral regulation in Sierra Leone but as a broader theoretical intervention into contemporary scholarship on constitutional governance, democratic legitimacy, and the future regulation of AI-mediated political communication.

C. Conclusion

This study concludes that Sierra Leone does not face a complete legal vacuum in relation to AI-generated electoral manipulation. The Constitution of Sierra Leone 1991, the Public Elections Act 2022, the Cyber Security and Crime Act 2021, and the Independent Media Commission Act 2020 provide technology-neutral rules capable of addressing particular manifestations of synthetic electoral interference where their statutory elements are satisfied. The principal deficiency is instead one of regulatory incompleteness: existing law addresses aspects of personation, false statements, undue influence, cyber-enabled impersonation, and media misconduct, but does not systematically regulate synthetic representation, deceptive authenticity, provenance, platform-mediated amplification, or time-sensitive electoral remedies. The answer to the first research question is therefore that Sierra Leone possesses partial but fragmented legal coverage of Synthetic Electoral Manipulation rather than an absence of applicable law.

The study's principal conceptual contribution is the formulation of Synthetic Electoral Manipulation (SEM) as a legally cognizable form of electoral interference defined by the convergence of synthetic representation, an electoral nexus, deceptive authenticity, legally relevant culpability, and actual or materially foreseeable democratic harm. This formulation distinguishes

SEM from ordinary misinformation without treating the use of artificial intelligence itself as sufficient to justify regulation. Correspondingly, the study does not claim that “electoral authenticity” is an autonomous constitutional right. It advances the narrower argument that electoral authenticity may function as a derivative constitutional interest where deceptive synthetic representations materially interfere with rights and institutions already protected by Sections 25 and 31–36 of the Constitution, including political expression, voting, electoral participation, and independent electoral administration.

In response to the second research question, the Synthetic Electoral Integrity Framework (SEIF) provides a constitutionally constrained architecture for addressing the residual deficiencies identified in the doctrinal analysis. Its five pillars classification, political AI transparency, platform accountability, narrowly defined electoral deepfake offences, and an emergency electoral response mechanism should be understood as complementary regulatory functions rather than isolated legislative proposals. Reform should therefore proceed incrementally: existing technology-neutral offences should be retained and clarified where they already apply, while new rules should be introduced only where identifiable gaps remain. Priority should be given to precise statutory definitions, provenance and disclosure requirements for materially synthetic electoral content, proportionate election-period platform duties, clearly delimited liability for culpable synthetic electoral interference, and expedited remedies for demonstrably harmful content whose effects may become irreversible before ordinary proceedings conclude. All such measures should remain subject to legality, necessity, proportionality, due process, Electoral Commission independence, and prompt judicial review.

The broader significance of the study lies in demonstrating that the central challenge posed by generative AI to electoral law is not technological novelty alone, but the increasing capacity to manufacture apparently authentic political realities at scale. SEIF is therefore proposed as a context-sensitive framework for Sierra Leone and as an analytically transferable model for other emerging democracies confronting comparable regulatory tensions, rather than as a template for direct legal transplantation. Future empirical research should test how synthetic electoral content affects voter judgment and institutional trust and should evaluate the practical effectiveness of disclosure, platform-governance, and rapid-response mechanisms in different electoral environments.

REFERENCES

- Ahmed, S., Chandra, S., Jain, A., Wongmahesak, K., & Singh, B. (2025). Impact of AI-Generated Misinformation on Electoral Integrity and Public Trust. In *Democracy and Democratization in the Age of AI* (pp. 57–72). IGI Global. <https://doi.org/10.4018/979-8-3693-8749-8.ch004>
- Al-Khazraji, S. H., Saleh, H. H., Khalid, A. I., & Mishkhal, I. A. (2023). Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, 23, 429–441. <https://doi.org/10.55549/epstem.1371792>
- Amezaga, N., & Hajek, J. (2022). Availability of Voice Deepfake Technology and its Impact for Good and Evil. *Proceedings of the 23rd Annual Conference on Information Technology Education*, 23–28. <https://doi.org/10.1145/3537674.3554742>
- Balendra, S. (2024). *Free Speech in the Puzzle of Content Regulation* (Vol. 70). Springer Nature Switzerland. <https://doi.org/10.1007/978-3-031-75813-3>
- Baltezarević, R., Lović, V., & Baltezarević, I. (2025). Between Progress and Peril: The Role of Artificial Intelligence (AI) in Shaping Modern Political Communication. *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE)*, 13(3),

823–835. <https://doi.org/10.23947/2334-8496-2025-13-3-823-835>

- Basanta Vázquez, B., & Azurmendi, A. (2025). Digital platforms and right to information: from mere hosts to responsible actors. *Revista de Comunicación*. <https://doi.org/10.26441/RC24.1-2025-3641>
- Birrer, A., & Just, N. (2025). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. *New Media & Society*, 27(12), 6819–6838. <https://doi.org/10.1177/14614448241253138>
- Branford, J., Soulier, E., & Fichtner, L. (2025). Generative AI and Democratic Culture. *Philosophy & Technology*, 38(3), 123. <https://doi.org/10.1007/s13347-025-00953-x>
- Bruno, N., & Moriggi, S. (2025). Disinformation: History, Drivers, and Countermeasures. *Encyclopedia*, 5(4), 211. <https://doi.org/10.3390/encyclopedia5040211>
- Cal. Elec. Code § 20010. (2026). *California Elections Code §§ 20010–20012 (2026)*. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?article&chapter=1.&division=20.&lawCode=ELEC&part&title
- Cárdenas Gracia, J. (2014). Idea, Validation and Criticism of the Principle of Balancing. *Boletín Mexicano de Derecho Comparado*, 47(139), 65–100. [https://doi.org/10.1016/S0041-8633\(14\)70501-0](https://doi.org/10.1016/S0041-8633(14)70501-0)
- Cea, N., Seijas-Costa, R., & Ibáñez, D. B. (2025). *How is the Cybersphere Regulated in Spain? Regulations and Laws for the Regulation of User-Generated Content* (pp. 451–461). https://doi.org/10.1007/978-981-96-0426-5_39
- Celeste, E. (2025). Social media and digital constitutionalism. In *Routledge Handbook of Social Media, Law and Society* (pp. 187–206). Routledge. <https://doi.org/10.4324/9781003252740-20>
- Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753. https://scholarship.law.bu.edu/faculty_scholarship/640
- Chrysogonos, K., & Stratilatis, C. (2012). Limits of Electoral Equality and Political Representation. *European Constitutional Law Review*, 8(1), 9–32. <https://doi.org/10.1017/S1574019612000028>
- Constitution of Sierra Leone. (1991). *The Constitution of Sierra Leone, 1991 (Act No. 6 of 1991)*. Parliament of Sierra Leone.
- Cupać, J., & Sienknecht, M. (2024). Regulate against the machine: how the EU mitigates AI harm to democracy. *Democratization*, 31(5), 1067–1090. <https://doi.org/10.1080/13510347.2024.2353706>
- Curran, L. (2022). Delaying Justice. In *Australian Courts* (pp. 143–168). Springer International Publishing. https://doi.org/10.1007/978-3-031-19063-6_7
- Cyber Security and Crime Act. (2021). *Sierra-Leone-Cyber-Crime-Act*.
- De Gregorio, G. (2022). *Digital Constitutionalism in Europe*. Cambridge University Press. <https://doi.org/10.1017/9781009071215>
- Diakopoulos, N., & Johnson, D. (2021). Anticipating and addressing the ethical implications of deepfakes in the context of elections. *New Media & Society*, 23(7), 2072–2098.

<https://doi.org/10.1177/1461444820925811>

- Dressel, B. (2012). The judicialization of politics in Asia: Towards a framework of analysis. In *The Judicialization of Politics in Asia* (pp. 15–28). Routledge. <https://doi.org/10.4324/9780203115596-6>
- Dziedzic, M. (2025). Combating Disinformation in the Context of Selected Regulations of the Digital Services Act and the Artificial Intelligence Act. *PRAWO i WIEŻ*, 53(6). <https://doi.org/10.36128/PRIW.VI53.1103>
- Edwards, L. M. (2019). “A Country Proud to be Democratic”: Demanding Democracy in Nineteenth-Century Chile. *The Americas*, 76(4), 585–605. <https://doi.org/10.1017/tam.2019.72>
- Eskiadi, I. G., & Panagiotou, N. (2025). The Impact of Social Media and Digital Campaigns. In *Understanding Voter Behavior With Predictive Modeling* (pp. 399–444). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3373-1037-4.ch013>
- European Union AI Act. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 a....* <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Ferrara, E. (2025). Charting the landscape of nefarious uses of generative artificial intelligence for online election interference. *First Monday*. <https://doi.org/10.5210/fm.v30i6.14188>
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Goswami, P., & Sachdeva, N. (2025). AI and electoral integrity. In *AI and the Future of Democracy* (pp. 126–144). Chapman and Hall/CRC. <https://doi.org/10.1201/9781003594185-8>
- Green, J. M., Sarrafzadeh, A., & Anwar, M. (2025). Critique of Networked Election Systems: A Comprehensive Analysis of Vulnerabilities and Security Measures. *Information*, 17(1), 10. <https://doi.org/10.3390/info17010010>
- Greenstein, S., & Zamboni, M. (2025). Navigating the legislative dilemma: evaluating the EU AI Act’s approach to regulating emerging technologies. *The Theory and Practice of Legislation*, 13(3), 312–352. <https://doi.org/10.1080/20508840.2025.2513177>
- Hammouri, J. A. (2024). The Criminal Liability of Artificial Intelligence Entities. *Pakistan Journal of Life and Social Sciences (PJLSS)*, 22(2). <https://doi.org/10.57239/PJLSS-2024-22.2.00662>
- Hanna, E., Zahr, E. A., Samrout, K., & Bakir, N. (2026). Technical Framework for Combating Deepfake Identity Fraud in E-Government Services. *2026 14th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. <https://doi.org/10.1109/ISDFS69419.2026.11458925>
- Helberger, N. (2020). The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power. *Digital Journalism*, 8(6), 842–854. <https://doi.org/10.1080/21670811.2020.1773888>

- Independent Media Commission Act. (2020). *The Independent Media Commission Act*.
- Jayakumar, S., Ang, B., & Anwar, N. D. (2021). Fake News and Disinformation: Singapore Perspectives. In *Disinformation and Fake News* (pp. 137–158). Springer Singapore. https://doi.org/10.1007/978-981-15-5876-4_11
- Jumhadi, H., & Dewi Heniarti, D. (2025). Misuse of Artificial Intelligence in Cybercrime: Criminal Liability and Electoral Integrity. *Jurnal Daulat Hukum*, 8(4), 967. <https://doi.org/10.30659/jdh.v8i4.50286>
- Karanja, J. M., & Nzau, T. (2026). The Emergence of AI Deepfakes and Their Impact on Strategic Crisis Communication: Practitioners' Perspectives From Kenya. *Journal of Contingencies and Crisis Management*, 34(1). <https://doi.org/10.1111/1468-5973.70140>
- Khanjani, Z., Watson, G., & Janeja, V. P. (2023). Audio Deepfakes: A Survey. *Frontiers in Big Data*, 5. <https://doi.org/10.3389/fdata.2022.1001063>
- Kopecky, S. (2024). *Challenges of Deepfakes* (pp. 158–166). https://doi.org/10.1007/978-3-031-62281-6_11
- Kučs, A. (2025). Freedom of Expression and Positive Obligations of the State in Social Media. In *Human Rights in the Digital Domain* (pp. 159–174). Cambridge University Press. <https://doi.org/10.1017/9781009606295.013>
- Łabuz, M. (2026). *Toward Transparency of Synthetic Media: EU Regulatory Perspective and Its Implications* (pp. 451–470). https://doi.org/10.1007/978-3-032-07605-2_22
- Lin, X. (2025). Protecting AI-Generated Images as Works of Fine Art in China: Magnifying the Legacy of Art to Copyright. *Law, Technology and Humans*, 7(1), 107–126. <https://doi.org/10.5204/lthj.3825>
- Luebke, S. M. (2021). Political Authenticity: Conceptualization of a Popular Term. *The International Journal of Press/Politics*, 26(3), 635–653. <https://doi.org/10.1177/1940161220948013>
- Maniyal, V., & Kumar, V. (2024). Unveiling the Deepfake Dilemma: Framework, Classification, and Future Trajectories. *IT Professional*, 26(2), 32–38. <https://doi.org/10.1109/MITP.2024.3369948>
- Marah, T. S. (2026a). Disinformation as a Weapon: Legal Limits of Cognitive Warfare Under International Humanitarian Law. *Cogent Social Sciences*, 12(1). <https://doi.org/10.1080/23311886.2026.2687180>
- Marah, T. S. (2026b). Judicial Reform and Human Security in West Africa: Comparative Lessons from Ghana and Sierra Leone. *Gloria Justitia*, 6(1), 331–340. <https://doi.org/10.25170/GLORIAJUSTITIA.V6I1.7907>
- Mbithi, A., & Kijima, Y. (2026). Rent Extraction and Political Accountability: Evidence From Audit Impact in Kenya. *Review of Development Economics*, 30(1), 255–287. <https://doi.org/10.1111/rode.13265>
- Minnesota Legislature. (2025). *Minnesota Statutes § 609.771: Use of deep fake technology to influence election*. Office of the Revisor of Statutes. <https://www.revisor.mn.gov/statutes/cite/609.771>
- Miranda Romero, A. E., Mera Cedeño, M. J., & Illicachi Guznay, J. (2025). Deepfakes as a Strategy to Spread Misinformation on Social Media During Ecuador's Election Campaigns.

- Revista de Ciencias Sociales*. <https://doi.org/10.31876/rcs.v31i4.44850>
- Norris, P. (2014). *Why Electoral Integrity Matters*. Cambridge University Press. <https://doi.org/10.1017/CBO9781107280861>
- Núñez Rocha, H. (2025). Artificial Intelligence and Copyright Law. Notes on Content Generation. *Boletín Mexicano de Derecho Comparado*, e20220. <https://doi.org/10.22201/ijj.24484873e.2025.174.20220>
- Paris, B., & Donovan, J. (2019). *Deepfakes and Cheap Fakes the Manipulation of Audio And Visual Evidence*. <https://datasociety.net/research/>
- Parliamentary Elections Act. (1954). *Singapore. (1954). Parliamentary Elections Act 1954. Singapore Statutes Online, Attorney-General's Chambers*. <https://sso.agc.gov.sg/Act/PEA1954>
- Pollicino, O., & Romeo, G. (Eds.). (2016). *The Internet and Constitutional Law*. Routledge. <https://doi.org/10.4324/9781315684048>
- Pooja Raj. (2025). The Impact of Deepfake Technology on Elections and Democratic Trust. *Indian Journal of Law*, 3(6), 56–64. <https://doi.org/10.36676/ijl.v3.i6.137>
- Protection from Online Falsehoods and Manipulation Act. (2019). *Act 2019 Act 18 of 2019 (Singapore)*. <https://sso.agc.gov.sg/Act/POFMA2019>
- Public Elections Act. (2022). *Act No. 17 of 2022 (Sierra Leone)*. <https://sierralii.gov.sl/akn/sl/act/2022/17/eng%402022-09-20>
- Puccinelli, O. R. (2025). Disinfodemic Threats. Real, False, and Fake News. In *Human Rights in the Digital Domain* (pp. 199–240). Cambridge University Press. <https://doi.org/10.1017/9781009606295.015>
- Regulation (EU) 2022/2065. (2022). *European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1*. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- Rocha, T. M. (2026). Digital Services Act: Towards the Digital Rule of Law. In *A Digital Europe for Citizens* (pp. 189–214). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-02500-5_11
- Romanishyn, A., Malyska, O., & Goncharuk, V. (2025). AI-driven disinformation: policy recommendations for democratic resilience. *Frontiers in Artificial Intelligence*, 8. <https://doi.org/10.3389/frai.2025.1569115>
- Rouméas, R. (2022). The Forced Passage of Law. Victims of Correctionalized Crimes Facing Professional Management of Judicial Delays. *Droit et Société*, N° 111(2), 269–288. <https://doi.org/10.3917/drs1.111.0269>
- Rubio Núñez, R. (2025). Does Artificial Intelligence Redefine Election Campaigns and Their Democratic Effects? *Revista de Derecho Político*, 122, 65–102. <https://doi.org/10.5944/rdp.122.2025.44742>
- Sam, S. (2019). Towards a New Public Sphere for Political Inclusion: Mobile Media and the Reshaping of Local Governance Landscapes in Sierra Leone. *Information Development*, 35(1), 135–149. <https://doi.org/10.1177/02666666917735361>
- Shaholli, M. (2025). Social Media as a Tool for Political Mobilization and Public Debate.

- Interdisciplinary Journal of Research and Development*, 12(1 S1), 192.
<https://doi.org/10.56345/ijrdv12n1s125>
- Slater, J., & Watt, B. (2015). In Defense of Democracy: The Criminalization of Impersonation. *Election Law Journal: Rules, Politics, and Policy*, 14(2), 165–185.
<https://doi.org/10.1089/elj.2015.0307>
- Soñeca, V. (2025). Risks and Challenges of Deepfakes in National and European Parliament Elections. In *Combatting Misinformation and Global Nation's False Narratives Through Education* (pp. 149–172). IGI Global. <https://doi.org/10.4018/979-8-3693-9601-8.ch006>
- Stavridou, V. (2025). AI-Driven Electoral Strategies. In *Understanding Voter Behavior With Predictive Modeling* (pp. 469–512). IGI Global Scientific Publishing.
<https://doi.org/10.4018/979-8-3373-1037-4.ch015>
- Steinebach, M., Wache, M., & Berchtold, W. (2026). Marking AI-Generated Content in Accordance with the EU AI Act. *Information – Wissenschaft & Praxis*, 77(2–3), 103–107.
<https://doi.org/10.1515/iwp-2026-2004>
- Tan, N., & Grofman, B. (2018). Electoral Rules and Manufacturing Legislative Supermajority: Evidence from Singapore. *Commonwealth & Comparative Politics*, 56(3), 273–297.
<https://doi.org/10.1080/14662043.2018.1468238>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media + Society*, 6(1). <https://doi.org/10.1177/2056305120903408>
- Van De Velde, J. (2021). The Dangers of Forceful Countermeasures as a Response to Cyber Election Interference. In *Defending Democracies* (pp. 215–238). Oxford University Press New York. <https://doi.org/10.1093/oso/9780197556979.003.0011>
- van Ham, C. (2020). Electoral Integrity. In R. Rohrschneider & J. Thomassen (Eds.), *The Oxford Handbook of Political Representation in Liberal Democracies* (pp. 112–133). Oxford University Press. <https://doi.org/10.1093/oxfordhb/9780198825081.013.5>
- Visnjic, D. (2025). *Generative Models and Deepfake Technology: A Qualitative Research on the Intersection of Social Media and Political Manipulation* (pp. 75–80).
https://doi.org/10.1007/978-3-031-79086-7_7
- Vujicic, J. (2025). *Analysis of Proposed Artificial Intelligence Regulations: Perspectives from the United States, China, and the European Union* (pp. 173–194). https://doi.org/10.1007/978-3-031-86330-1_10
- Wardle, C., & Derakhshan, H. (2017). *Information Disorder: Toward an interdisciplinary framework for research and policy making*. *Information Disorder Toward an interdisciplinary framework for research and policymaking*. www.coe.int
- Washington State Legislature. (2025). *Revised Code of Washington § 29B.35.010: Action by candidate for relief and damages Defenses*.
https://lawfilesex.t.leg.wa.gov/Law/RCWArchive/2024/RCW_29B.35_CHAPTER.htm
- Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, 9(11), 39–52. <https://doi.org/10.22215/timreview/1282>
- Zafarullah, H., & Nughat, S. (2026). Regulatory Control and Self-Censorship in Social Media: Stifling Freedom of Expression in Bangladesh. *Journal of Asian and African Studies*.

<https://doi.org/10.1177/00219096261437744>

Zheng, G., Shu, J., & Li, K. (2025). Regulating Deepfakes Between Lex Lata and Lex Ferenda—a Comparative Analysis of Regulatory Approaches in The U.S., the EU and China. *Crime, Law and Social Change*, 83(1), 1. <https://doi.org/10.1007/s10611-024-10197-z>