

**REGULATING ALGORITHMIC DISINFORMATION IN ELECTORAL
DEMOCRACIES: THE ROLE OF SOCIAL MEDIA ALGORITHMS IN KENYA'S
ELECTORAL DEMOCRACY**

Submitted in partial fulfillment of the requirements of the Bachelor of Laws Degree, Strathmore
University Law School

By

Sandra Katunge Musyoka

139125

Prepared under the supervision of

James Nyiha

March 2025

Word count (14899)

Declaration

I, SANDRA KATUNGE MUSYOKA, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.



Signed:

Date: 23rd March 2025

This dissertation has been submitted for examination with my approval as University Supervisor.



Signed:

Supervisor's Name: **James Nyiha**

Date: **24th March 2025**

Acknowledgements

I extend my deepest gratitude to my supervisor, Mr. Nyiha, for his guidance, feedback, and support as I conducted research and write this paper. whose guidance, feedback, and unwavering support have been invaluable throughout this research. His insights and expertise have significantly contributed to shaping the direction and quality of this work.

I am deeply appreciative of my family, Ruby and Mum, for their endless encouragement, motivation, and unwavering support. I would also like to express my heartfelt gratitude to my friends, Elsie, Cindy, Njambi, and Abi, for their unwavering support and motivation. Their encouragement and companionship have been instrumental in helping me stay focused and determined.

List of Legal Instruments

Computer Misuse and Cybercrimes Act (No. 5 of 2018)

Constitution of Kenya (2010)

Data Protection Act (No. 24 of 2019)

Digital Services Act (2022)

Elections Act (No.24 of 2011)

EU AI Act

Independent Electoral and Boundaries Commission Act (No. 9 of 2011)

Kenya Information and Communication (Amendment) Bill (Bill No. 61 of 2019)

Kenya Information and Communications Act (KICA) (No. 41A of 2013)

Kenya National Artificial Intelligence (AI) Strategy (Draft, 2025-2030)

National Cohesion and Integration Act (No.12 of 2008)

Political Advertising Regulation (2023)

List of Abbreviations

AI	Artificial Intelligence
CAK	Communications Authority of Kenya
CMCA	Computer Misuse and Cybercrimes Act
DEIC	Digital Election Integrity Commission
DPA	Data Protection Act
DSA	Digital Services Act
DSC	National Digital Services Coordinators
EBDS	European Board for Digital Services
GANs	Generative Adversarial Networks
GPT	Generative Pre-trained Transformer
ICT	Information and Communication Technology
IEBC	Independent Electoral and Boundaries Commission
KICA	Kenya Information and Communications Act
NCIC	National Cohesion and Integration Commission
UNESCO	United Nations Educational, Scientific and Cultural Organization
VAEs	Variational Autoencoders

Abstract

Algorithmic disinformation poses a growing challenge to electoral democracy, particularly in Kenya, where social media platforms have become central to political discourse. This study explores the role of social media algorithms in amplifying false information and the inadequacies of Kenya's current legal and regulatory framework in addressing this issue. The primary objective of this study is to analyze the effectiveness of Kenya's legal framework in regulating algorithmic disinformation, identify its limitations, and propose targeted reforms to safeguard electoral integrity. It focuses on Kenya's electoral processes, examining how social media algorithms contribute to disinformation and evaluating legal and policy responses. It also incorporates comparative insights from international regulatory frameworks.

The research employs a qualitative approach, including legal analysis, comparative studies, and a review of academic literature. It examines relevant legislation, case law, and regulatory practices in Kenya and selected jurisdictions. The study reveals significant gaps in Kenya's legal framework, including the absence of a clear definition of algorithmic disinformation, lack of platform liability, and an uncoordinated regulatory approach. These shortcomings allow disinformation to thrive, undermining democratic processes. The findings highlight the urgent need for comprehensive regulatory measures.

This study proposes several reforms, including defining algorithmic disinformation within the legal framework, implementing mandatory algorithmic audits, establishing a centralized body for digital election integrity, and enforcing transparency and accountability requirements for social media platforms. These measures aim to enhance oversight and mitigate the risks posed by disinformation, ultimately strengthening electoral democracy in Kenya.

Table of Content

CHAPTER 1: INTRODUCTION	1
1.0 Background of the problem	1
1.1 Statement of the problem	4
1.2 Purpose of the study	5
1.3 Research questions.....	5
1.4 Hypothesis.....	5
1.5 Rationale of the study	5
1.6 Theoretical Framework/ Conceptual Framework	6
1.6.1 Marketplace of Ideas Theory	6
1.6.2 Democratic Theory	7
1.8 Methodology	10
1.9 Limitation.....	11
2.0 Chapter breakdown	11
CHAPTER TWO: THEORETICAL AND CONCEPTUAL FOUNDATIONS	12
2.1 Introduction.....	12
2.2 Disinformation and Misinformation	12
2.3 The Role of Social Media in Democracy.....	13
2.3.1 Social Media Algorithms	18
2.4 Algorithmic Disinformation and Democracy	22

2.5 Conclusion	24
CHAPTER 3: LEGAL AND REGULATORY FRAMEWORK GOVERNING DISINFORMATION IN KENYA	26
3.0 Introduction.....	26
3.1 The Legal and Institutional Governing Algorithmic Disinformation in Kenya	27
3.1.1 Legal Framework in Kenya	27
3.2 The Inadequacies of the Legal Framework on Algorithmic Disinformation.....	33
3.2.1 Absence of a legal definition of algorithmic disinformation	33
3.2.2 No Specific Regulation for Social Media Algorithms in Political Content Moderation	34
3.2.3. Lack of Regulations Governing Electoral Algorithmic Disinformation.....	34
3.2.4 No Platform Liability for Algorithmic Disinformation	35
3.2.5 Lack of Coordinated Regulation	35
3.3 Legislative Attempts and Their Failures.....	36
3.4 Comparative Analysis.....	37
3.4.1 Overview of the Existing Laws.....	37
3.4.2 Comparison with Kenya’s Regulatory System	38
3.5 Conclusion	39
CHAPTER 4: RECOMMENDATIONS.....	40
4.0 Introduction.....	40
4.1 Defining Algorithmic Disinformation	40
4.2 Regulating Social Media Algorithms.....	41

4.3 Creating a Centralized Body	42
4.4 Transparency and Reporting Requirements	43
4.5 Conclusion	44
CHAPTER 5: CONCLUSION	45
Books	47
Chapters in Books	47
Hard Copy Journals.....	47
Online Journal Articles	47
Reports	49
Online Sources	49
Working Papers.....	49

CHAPTER 1: INTRODUCTION

1.0 Background of the problem

Manipulating the truth has been a persistent occurrence throughout history, adapting to different forms of communication over time.¹ The rise of technological advancements in the digital age has profoundly transformed various aspects of life, including how information is consumed and spread.² Information and Communication Technology (ICT), particularly social media has revolutionised public engagements and political discourse. This is done by providing access to information and new platforms for political participation.³ In an era where communication knows no bounds, the internet has become a powerful tool for self-expression and connection on a global scale. However, if left unchecked it will create a space of harmful and false information.

The presence of social media in electoral processes has proved to be a double-edged sword. On the one hand, technology has enabled broader public engagement, transparency and accountability, and ensuring that the average voter is more informed. On the other hand, social media has been used as a tool to spread disinformation and misinformation, which undermines electoral integrity.⁴ Misinformation is defined as false or misleading information disseminated with no intent to deceive while disinformation is inaccurate information which is intentionally created and disseminated with the intent to mislead the public.⁵

Democracy, as a system of good governance, relies on the notions of accountability, transparency and active participation of citizens in decision-making.⁶ A robust democracy relies on public

¹ Bontridder N and Poulet Y, 'The role of artificial intelligence in disinformation' *Data & policy*, 2021, e32-2 - <https://doi.org/10.1017/dap.2021.20> - on 22 December 2024.

² The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age , *Protecting electoral integrity in the digital age*, 2020, 13.

³ Sugow A, 'The right to be wrong: Examining the (Im) possibilities of regulating fake news while preserving the freedom of expression in Kenya' *Strathmore Law Review*, 2019, 42 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3623716 on 13 August 2024.

⁴ Ndlela M, 'Algorithms, bots and elections in Africa: how social media influences political choices' *The conversation*, 30 March 2022 <https://theconversation.com/algorithms-bots-and-elections-in-africa-how-social-media-influences-political-choices-179121> on 20 January 2025.

⁵ Martin-Rozumilowicz B and Kuzel R, 'Social media, disinformation and electoral integrity' IFES Working Paper, 3, <https://www.ifes.org/publications/social-media-disinformation-and-electoral-integrity> on 28 August 2024.

⁶ Margetts H, 'Rethinking democracy with social media,' 90 *The Political Quarterly* S1, 2018, 107.

discourse, the free exchange of ideas, and unlimited access to accurate and truthful information.⁷ Elections are a cornerstone of democracy, providing a mechanism for citizens to choose their leaders and hold them accountable.⁸

In recent years, social media has been used to influence public opinion, distort electoral outcomes, and exacerbate political division.⁹ However, historically, disinformation is not a new phenomenon in political elections. Manipulation of voters through the dissemination of false information can be traced back to early forms of media such as print media and radio broadcasting.¹⁰ However, social media has amplified these effects.

Algorithmic disinformation, a new and evolving threat, refers to the dissemination of false and misleading information using AI-driven recommendation and generative algorithms.¹¹ Social media algorithms have fundamentally reshaped the way individuals consume and engage with information.¹² By tracking user interactions, algorithms curate content that aligns with past behaviour, reinforcing pre-existing beliefs and preferences.¹³ Furthermore, algorithms often prioritise content that elicits strong emotional responses, as they will lead to higher engagement with particular content.¹⁴ Misinformation and disinformation frequently possess these characteristics, making them more likely to be promoted by algorithms. These algorithms are designed to create an “echo chamber” where users are predominately exposed to information that aligns with their beliefs.¹⁵ Unlike traditional forms of media, these algorithms operate invisibly,

⁷ Olaniran B and Williams I, ‘Social media effects: Hijacking democracy and civility in civic engagement’ *Platforms, Protests, and the Challenge of Networked Democracy*, 2020, 79 [doi:10.1007/978-3-030-36525-7_5](https://doi.org/10.1007/978-3-030-36525-7_5) on 28 October 2024.

⁸ Olaniran B and Williams I, ‘Social media effects: Hijacking democracy and civility in civic engagement,’ 78.

⁹ Olaniran B and Williams I, ‘Social media effects: Hijacking democracy and civility in civic engagement,’ 82.

¹⁰ Rutenburg I and Sugow A, ‘Regulation of the social media in electoral democracies: A case of Kenya’ Vol VII(I) *SOAS Law Journal*, 2020, 302.

¹¹ Sun H, ‘Regulating algorithmic disinformation’ Volume 46 Issue No.4 *The Columbia Journal of Law & The Arts*, 2013, 373.

¹² Ndlela M, ‘Algorithms, bots and elections in Africa: how social media influences political choices’.

¹³ Sun H, ‘Regulating algorithmic disinformation’, 374.

¹⁴ Chalke S and Mishra D, ‘Studying the impact of social media algorithms on the spread of misinformation and its effects on society’ *International Journal of Advanced Research in Science Communication and Technology*, 2023, 354-

<https://www.researchgate.net/publication/374300955_Studying_the_Impact_of_Social_Media_Algorithms_on_the_Spread_of_Misinformation_and_its_Effects_on_Society>- on 28th October 2024.

¹⁵ Margetts H, ‘Rethinking democracy with social media,’ 110.

making it difficult to determine the rationale behind content prioritization.¹⁶ Consequently, social media users are often unaware of the extent to which their digital experiences are shaped by these systems. This raises concerns about transparency, bias, and the broader implications of these algorithms.

In Kenya, the influence of technology in electoral processes has been a critical area of concern, especially in the previous election years. Since gaining independence in 1963, Kenya has experienced election disputes and political violence based on tribal lines. In 2007, there was a significant loss of life and displacement of many Kenyan citizens due to the volatile nature of Kenyan politics which triggered atrocious humanitarian crimes.¹⁷ In particular, the 2013 and 2017 elections demonstrated the influence of social media in shaping the electoral process. Social media became a critical tool for political campaigns, as political parties and candidates used these platforms to mobilize voters.¹⁸

The 2017 elections marked a critical turning point in the use of social media in elections. This is evident from the emergence of extensive data harvesting and targeted disinformation campaigns.¹⁹ Firms like Cambridge Analytica exploited personal data to target voters with tailored political propaganda.²⁰ The campaigns during these elections utilized automated systems and bot networks to amplify narratives, leading to erasure of public trust in the election process.²¹ The 2022 elections further amplified these challenges with the rise of AI-powered disinformation tools.²² Coordinated bot networks and falsified opinion polls were used to spread misleading information about election outcomes, deepening political polarization.²³

To address these challenges, Kenyan policymakers have created regulations to address the issue

¹⁶ Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya' Volume 3 Issue 1, *Journal of Intellectual Property and Information Technology Law*, 2023, 207.

¹⁷The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age , *Protecting electoral integrity in the digital age*, 2020, 53.

¹⁸The Report of the Kofi Annan Commission on Elections and Democracy in the Digital Age , *Protecting electoral integrity in the digital age*, 53-54.

¹⁹ KICTANet, *Fake news, dangerous speech and the elections: Talk to NCIC – KICTANet community engagement report*, 2017, 3.

²⁰ Rutenburg I and Sugow A, 'Regulation of the social media in electoral democracies: A Case of Kenya,' 331.

²¹ Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya'. 212.

²² Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya'. 212.

²³ Agbele F, 'Disinformation and misinformation during Kenya's 2022 election: Implications for voter confidence in the electoral process', *MegaTrends Afrika*, 2023, 3.

of misinformation and electoral misconduct. The Constitution of Kenya is the cornerstone of Kenya's democratic principles and values. It enshrines freedom of expression in Article 33 which grants every Kenyan citizen liberties as well as certain obligations and exceptions when it comes to harming or jeopardising the safety of others.²⁴

Additionally, the Kenya Information and Communications (Amendment) Act of 2013, and the Computer Misuse and Cyber Crimes Act of 2018 criminalise misinformation and the publication of false information.²⁵

However, the dissemination of disinformation, especially during elections raises concerns about whether the legal framework adequately balances the need to protect democratic processes while upholding fundamental freedoms such as the freedom of speech.²⁶ Furthermore, the legal landscape in Kenya has struggled to keep pace with the rapid evolution of digital technologies and the sophisticated nature of algorithmic disinformation. Not all fake news is inherently harmful; there are instances where misinformation contributes to society positively. Nevertheless, disinformation distorts public perception and undermines democratic integrity.

The challenges experienced in Kenya during the 2013, 2017 and 2022 elections bring into question whether the current regulatory framework addresses the harmful impacts of fake news while safeguarding the freedom of expression and access to information.

1.1 Statement of the problem

Disinformation is not a new phenomenon in electoral politics, however, the rise of automated algorithms has increased its reach and impact. Unlike traditional disinformation and misinformation, algorithmic disinformation uses automated mechanisms to rapidly amplify falsehoods, shaping public perceptions in real time. This underscores the urgent need for effective regulation to counter the harmful effects of algorithmic disinformation.

²⁴ Article 33, *Constitution of Kenya* (2010).

²⁵ Section 22, *Computer Misuse and Cyber Crimes Act* (No. 5 of 2018).

²⁶ Mudavadi K, Matanji F, Diop L, Tully M and Madrid-Morales D, 'Stakeholder perceptions of regulatory responses to misinformation in Kenya and Senegal' *Sage Journals*, 2024, 3-
<https://journals.sagepub.com/doi/10.1177/14648849241255935> on 25 August 2024.

1.2 Purpose of the study

This study aims to achieve the following objectives:

1. Analyze the current legal and regulatory frameworks in Kenya that address election-related disinformation and their effectiveness in preventing mass atrocity crimes.
2. Investigate how social media algorithms contribute to the dissemination of disinformation in Kenya's electoral context, and evaluate the impact of these algorithms on electoral integrity and political stability.
3. Propose practical recommendations for enhancing legal and policy measures to better address election-related disinformation and mitigate associated risks.

1.3 Research questions

This study seeks to answer the following research questions:

1. What are the limitations of the current legal and regulatory frameworks in Kenya regarding election-related disinformation?
2. How do social media algorithms contribute to the spread of disinformation during electoral processes in Kenya?
3. What practical measures can be recommended to strengthen the legal and policy responses to election-related disinformation in Kenya?

1.4 Hypothesis

Although Kenya has established various legal and regulatory mechanisms to address election-related disinformation, these frameworks are inadequate in managing the sophisticated and evolving nature of algorithmic disinformation. This inadequacy contributes to heightened risks of mass atrocity crimes during electoral periods. By addressing these legal gaps and adapting regulatory approaches, it is possible to better mitigate the threats posed by disinformation and enhance electoral stability.

1.5 Rationale of the study

As it stands, the internet is a powerful tool for communication and dissemination of information. The spread of algorithmic disinformation poses significant risks to individuals, communities and the democratic process as a whole. By evaluating the effectiveness of the existing legal frameworks, this study seeks to inform the general public specifically policymakers and scholars

about the need for alternative strategies to mitigate the harm caused by this misinformation while upholding the freedom of speech accorded to persons and democratic integrity.

Further, the findings of this study will add to the ongoing discourse surrounding content moderation and the role of government regulation in addressing the pressing issue of misinformation.

1.6 Theoretical Framework/ Conceptual Framework

1.6.1 Marketplace of Ideas Theory

John Stuart Mill's philosophy on freedom of speech, epitomized by the metaphor of the marketplace of ideas, posits that in a free and open exchange of opinions, truth will naturally emerge as the prevailing force.²⁷ According to Mill, allowing diverse viewpoints to contend in a metaphorical marketplace facilitates the discovery and dissemination of knowledge, leading to the advancement of society.²⁸ In this framework, the unfettered competition of ideas is expected to filter out falsehoods and elevate the most robust and verifiable propositions through public scrutiny and debate. However, while this theory underscores the intrinsic value of free expression, it encounters challenges in the modern context of disinformation.

In today's digital landscape, the proliferation of disinformation complicates the functioning of the marketplace of ideas. False narratives, deliberately crafted misinformation, and echo chambers on social media platforms can distort the marketplace, making it difficult for truth to prevail. Disinformation campaigns often exploit vulnerabilities in the information ecosystem, spreading misleading content at scale and undermining the public's ability to discern fact from fiction. Consequently, the marketplace of ideas, which relies on the assumption of equal access to information and the capacity for critical evaluation, faces significant hurdles in combatting the spread of falsehoods.

To address the challenge of disinformation within the framework of the marketplace of ideas, proactive measures are necessary. Promoting media literacy and critical thinking skills becomes imperative to empower individuals to navigate the complexities of the digital information

²⁷ Mill, J.S, *On Liberty*, Hackett Publishing, Indianapolis, 1978, 9.

²⁸ Mill, J.S, *On Liberty*, Hackett Publishing, Indianapolis, 1978, 10.

landscape effectively. By equipping citizens with the tools to assess the credibility of sources, recognize common tactics used to spread misinformation, and critically evaluate information, societies can bolster their resilience against the influence of falsehoods. Additionally, responsible platform governance and policy interventions are essential to mitigate the spread of disinformation while safeguarding the principles of free expression. Balancing the need to curb harmful misinformation with the protection of free speech rights presents a complex challenge that requires collaboration between stakeholders across sectors.

In essence, while the marketplace of ideas remains a foundational concept in understanding freedom of speech, its application in addressing disinformation necessitates a nuanced approach. By acknowledging the evolving dynamics of the digital information landscape and implementing targeted interventions, societies can uphold the principles of free expression while effectively combating the spread of harmful misinformation.

1.6.2 Democratic Theory

Democratic theory posits that democracy is based on the principles of **political equality, collective self-rule** and **the protection of fundamental rights and freedoms**.²⁹ In a democratic society, citizens are expected to participate in decision-making processes, engage in public discourse, and hold their leaders accountable.³⁰ However, the spread of disinformation can erode these democratic principles by distorting public perceptions and undermining trust in democratic institutions.

Participatory democracy, a key aspect of democratic theory, emphasizes the direct involvement of citizens in political decision-making.³¹ This form of democracy relies on the active engagement of individuals in discussions and decision-making processes, ensuring that their voices are heard and considered in the governance of their communities.³² The role of social media in participatory

²⁹Munck G, 'Democratic theory and concept formation: ideals and realistic standards', 2023, 139, <https://ssrn.com/abstract=436518> on 20 January 2025.

³⁰ Munck G, '*Democratic theory and concept formation: ideals and realistic standards*', 2023, 147.

³¹ Olaniran B and Williams I, 'Social media effects: Hijacking democracy and civility in civic engagement,' 79.

³²Bobbio L, 'Designing effective public participation' *Policy and Society*, 2019, 45-
<<https://academic.oup.com/policyandsociety/article/38/1/41/6403983>>-on 28 October 2024.

democracy is significant, as it provides a platform for citizens to express their opinions, mobilize for causes, and engage in public discourse.³³

However, the introduction of social media has also brought challenges to participatory democracy. While social media platforms enable widespread participation, they can also facilitate the spread of disinformation and fragmented ideas. Disinformation campaigns can distort public perceptions, leading to the spread of false narratives and undermining the quality of public discourse.³⁴ This can result in a misinformed electorate, which is less capable of making rational decisions and holding leaders accountable. Furthermore, social media can create echo chambers, where individuals are exposed only to information that reinforces their existing beliefs.³⁵ This can lead to political polarization and the spread of populism, as fragmented ideas replace coherent discussions.

To address these challenges, democratic theory advocates for measures that enhance the quality of information available to citizens and promote transparency and accountability in the dissemination of information. This includes promoting media literacy, implementing robust fact-checking mechanisms, and ensuring that social media platforms are held accountable for the content they host.³⁶ By fostering an informed and engaged citizenry, democratic societies can better withstand the challenges posed by algorithmic disinformation.

In essence, the democratic theory provides a comprehensive framework for understanding the impact of algorithmic disinformation on electoral democracies. It underscores the need for an informed citizenry and the protection of democratic principles. By addressing the challenges posed by disinformation and enhancing the quality of public discourse, democratic societies can safeguard the integrity of their electoral processes and ensure that the will of the people is accurately reflected in the outcomes.

1.7 Literature Review

³³Berelson B, 'Democratic theory and public opinion' *The Public Opinion Quarterly*, 1952, 323-
<https://www.jstor.org.ezproxy.library.strathmore.edu/stable/pdf/2745778.pdf?refreqid=fastly-default%3Ab42e74ea4f4624725a6cf1623f29bea9&ab_segments=0%2Fbasic_expensive_solr_cloud%2Fcontrol&initiator=&acceptTC=1>- on 28 December 2024.

³⁴ Margetts H, 'Rethinking democracy with social media,' 112.

³⁵ Margetts H, 'Rethinking democracy with social media,' 107.

³⁶ Berelson B, 'Democratic theory and public opinion,' 318.

Abdulmalik Sugow's article, *The Right to be Wrong: Examining the (Im)Possibilities of Regulating Fake News while Preserving Freedom of Expression in Kenya*, is a crucial article that offers an important analysis of the conflict between controlling disinformation and upholding freedom of expression in Kenya. Sugow examines Kenya's *Computer Misuse and Cybercrimes Act*, which criminalizes false information which infringes on fundamental democratic freedoms.³⁷ He contends that while legislative measures are necessary to curb harmful misinformation, vaguely defined regulations could be weaponized against political dissent.³⁸ This perspective is highly relevant to this research as it demonstrates the challenge of formulating legal responses to digital threats without compromising free speech. His analysis is pertinent to this study as it underscores the necessity of a regulatory system that effectively controls disinformation without undermining essential rights and freedoms.

Haochen Sun's article, *Regulating Algorithmic Disinformation*, presents a comparative analysis of how different jurisdictions have responded to algorithmic disinformation, particularly China and France.³⁹ This research is extremely relevant because it provides a comparative viewpoint that can guide the creation of successful regulatory solutions in Kenya by shedding light on how other jurisdictions are handling algorithmic disinformation. His study highlights the effectiveness of mandatory algorithmic transparency laws in preventing the spread of disinformation. This paper benefits from Sun's comparative approach, as it offers potential lessons that can be adapted to Kenya's digital governance landscape.

Ali Abdirahman's article, *Algorithmic Disinformation and Electoral Integrity in the Digital Age*, highlights the increased role of automated systems in distorting public discourse, manipulating electoral narratives and influencing voters' perception of electoral candidates.⁴⁰ By examining Kenya's 2017 and 2022 elections, Ikran demonstrates how social media algorithms and bot networks have been used to spread disinformation and misinformation at an unprecedented scale. He argues that social media platforms prioritize content that maximizes interaction through

³⁷ Sugow A, 'The Right to be wrong: Examining the (im)possibilities of regulating fake news while preserving the freedom of expression in Kenya' 23.

³⁸ Sugow A, 'The Right to be wrong: Examining the (im)possibilities of regulating fake news while preserving the freedom of expression in Kenya,' 36.

³⁹ Sun H, 'Regulating algorithmic disinformation,' 373.

⁴⁰ Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya', 206.

‘attention capture’ which often amplifies emotionally charged misinformation rather than factual reporting.⁴¹ This finding is crucial for this study as it highlights the structural vulnerabilities within digital ecosystems which allow disinformation to thrive. This aligns with the objectives of this paper, which seeks to analyze the intersection between disinformation and misinformation.

Isaac Rutenberg’s article, *Regulation of Social Media in Electoral Democracies: A Case of Kenya*, examines the role of social media in Kenya’s elections, particularly how digital platforms have intensified political instability.⁴² A key aspect of Rutenberg’s analysis is his argument that while social media enables political participation, it also creates vulnerabilities that malicious actors can exploit. He discusses the role of unregulated digital campaigns, emphasizing that Kenya lacks a cohesive strategy for tackling politically motivated disinformation. This research is particularly relevant as it highlights the urgency of regulatory reforms that address the risks posed by social media while ensuring platforms do not become tools of political suppression.

The reviewed literature collectively highlights the multifaceted nature of algorithmic disinformation and its impact on electoral democracy. Ikran’s research provides a foundational understanding of the mechanisms through which AI-driven disinformation spreads, while Sugow’s work underscores the tension between regulation and free speech in the Kenyan legal context. Rutenberg’s study establishes the role of social media in intensifying political instability, and Sun’s comparative analysis offers global perspectives on regulatory responses.

This research seeks to bridge this gap by assessing the effectiveness of current Kenyan regulations and proposing a balanced framework that mitigates the harms of algorithmic disinformation while upholding democratic values.

1.8 Methodology

This research will primarily utilize qualitative and doctrinal methodologies. The information will be sourced mainly from written laws, books, journal articles, legal commentaries, and other credible publications on the subject. Additionally, factual data may be gathered from reputable

⁴¹ Ikran A, ‘Exploring co-regulation as a solution to automated disinformation in Kenya’, 209.

⁴² Rutenburg I and Sugow A, ‘Regulation of the social media in electoral democracies: A case of Kenya’, 307-309.

newspaper publishers. Given the evolving nature of the issue, various judicial decisions and opinions will also be considered.

1.9 Limitation

The study faces several limitations that may impact the depth of the findings. First, the nature of misinformation presents a challenge as there may be discrepancies in reported numbers and statistics across various sources. This will affect the study as I will not go into the field to interact with social media users to understand the extent of government regulation on social media and how fake news affects them. The complexity of the challenge further poses a problem when identifying false information, specifically given the rapid growth of the internet and its users. Furthermore, due to the nature of social media, it keeps evolving each day and there could be new aspects that the study does not capture.

2.0 Chapter breakdown

Chapter One introduces the research topic by providing a background to the study. It outlines the statement of the problem, hypothesis, research objectives, research questions, methodology, literature review, and the significance of the study to the current legal system.

Chapter Two explores the theoretical and conceptual foundations of social media. It delves into the concepts of misinformation, disinformation, and algorithmic disinformation, offering a nuanced understanding of how these phenomena interact within electoral democracies. It further gives insights on the types of algorithms that contribute to the spread of the disinformation.

Chapter Three examines the legal framework governing social media regulation in Kenya. It provides a detailed analysis of key regulatory bodies. This chapter discusses the roles these institutions play in regulating media and social media in Kenya, especially during electoral processes. It critically evaluates existing laws highlighting their shortcomings in addressing the challenges posed by algorithmic disinformation.

Chapter Four offers a comparative analysis and policy recommendations that Kenya could adopt to tackle the challenges posed by algorithms. Chapter Five concludes the study by summarizing the key findings from the previous chapters.

CHAPTER TWO: THEORETICAL AND CONCEPTUAL FOUNDATIONS

2.1 Introduction

This chapter aims to provide a comprehensive understanding of the conceptual and theoretical foundations of algorithmic disinformation. By exploring key definitions, theoretical perspectives, and mechanisms through which algorithms propagate disinformation. Understanding these concepts is crucial for developing effective strategies to combat this form of disinformation.

2.2 Disinformation and Misinformation

Disinformation is the intentionally deceptive false or misleading information that is created, presented and disseminated to the public.⁴³ This information can cause public harm, including threats to public health, security and democratic processes.⁴⁴ Misinformation is false or misleading information spread without the intention to deceive.⁴⁵ Both disinformation and misinformation have significant impacts on information, however, disinformation is of particular concern due to its intentional nature. In this study, the focus on disinformation is crucial because the dissemination of this information is deliberate and often orchestrated to achieve certain goals such as influencing elections.⁴⁶

Several psychological tendencies contribute to the spread of misinformation and disinformation. One key factor is the role of cognitive biases, where individuals tend to seek out information that confirms their pre-existing beliefs.⁴⁷ This leads to selective exposure to information that aligns with one's views while disregarding information that contradicts them. This can create echo chambers, where individuals are only exposed to information that reinforces their beliefs, further entrenching misinformation and disinformation.⁴⁸

⁴³ Bontridder N and Poulet Y, 'The role of artificial intelligence in disinformation,'e32-2.

⁴⁴ European Commission, *Tackling Online Disinformation: A European Approach*, 2018.

⁴⁵ Bontridder N and Poulet Y, 'The role of artificial intelligence in disinformation,'e32-2.

⁴⁶Stepney E and Lally C, 'Disinformation: sources, spread and impact' *POSTnote*, 25 April 2024, 2-
<<https://post.parliament.uk/research-briefings/post-pn-0719/>>- on 22 December 2024.

⁴⁷ Ziemer C-T and Rothmund T, 'Psychological underpinnings of misinformation countermeasures: A systematic scoping review' *Journal of Media Psychology: Theories, Methods, and Applications*, 2024, 398-
<https://doi.org/10.1027/1864-1105/a000407> on 1 February 2025.

⁴⁸ Margetts H, 'Rethinking democracy with social media,'110.

Disinformation and misinformation can be disseminated through various channels, including traditional media, word of mouth, and digital platforms.⁴⁹ Several factors influence the mechanisms of their spread. Economic insecurity, rising extremism, and cultural shifts generate anxiety and provide a breeding ground for disinformation campaigns.⁵⁰ These campaigns often create a scenario where false information is mistaken for truth, while genuine content may be dismissed as fake.⁵¹ They exploit societal tensions, polarisation, and distrust to manipulate public opinion and foster societal discord.⁵² The creation of disinformation can be driven by political, ideological, or economic motives, with actors ranging from state-sponsored entities to individual opportunists.⁵³ This leads to distrust and the creation of social tension, which leads to the undermining of social institutions and eroding the integrity of elections.⁵⁴

Digital platforms in particular have become content aggregators and distributors, entering the news business without necessarily adopting the editorial frameworks and capabilities of traditional media outlets.⁵⁵ Their economic incentives lead them to capture a large user base by exploiting network effects and maximising user engagement, often preferring to disseminate quantity of information over quality.⁵⁶

2.3 The Role of Social Media in Democracy

Social media is defined as “a group of Internet applications...that allow the creation and exchange of user-generated content”.⁵⁷ These platforms enable users to create profiles, connect with others, and share various forms of content, including text images and videos.⁵⁸ These platforms are

⁴⁹ Chalke S and Mishra D, ‘Studying the impact of social media algorithms on the spread of misinformation and its effects on society,’ 356.

⁵⁰ European Commission, *Tackling Online Disinformation: A European Approach*, 2018.

⁵¹ Bontridder N and Pouillet Y, ‘The role of artificial intelligence in disinformation,’ e32-4.

⁵² Ikran A, ‘Exploring co-regulation as a solution to automated disinformation in Kenya’, 213.

⁵³ European Commission, *Tackling Online Disinformation: A European Approach*, 2018.

⁵⁴ European Commission, *Tackling Online Disinformation: A European Approach*, 2018.

⁵⁵ Bontridder N and Pouillet Y, ‘The role of artificial intelligence in disinformation,’ e32-4.

⁵⁶ Heitmayer M, ‘The second wave of attention economics: Attention as a universal symbolic currency on social media and beyond’ *Interacting with Computers*, 2024, 19- <https://doi.org/10.1093/iwc/iwae035> on 23 January 2025.

⁵⁷ Kaplan A and Haenlein M, ‘Users of the world, unite! The challenges and opportunities of social media’ *Business Horizons*, 2010, 53, 61—<https://doi.org/10.1016/j.bushor.2009.09.003> on 1 February 2025.

⁵⁸ Boyd M and Ellison B, ‘Social network sites: definition, history, and scholarship’ 13 *Journal of Computer-Mediated Communication* 1, 2007, 211.

characterised by their ability to create profiles, make transverse relationships and facilitate user interactions.⁵⁹

The primary goal of these platforms is to capture and retain the attention of its users.⁶⁰ This is based on the economics of attention where the more individuals use social platforms, the more economic gain these platforms generate.⁶¹ These platforms generate revenue from advertising and leveraging user data to create attractive content. The more time users spend on a platform, the more data is collected, the more valuable the platform becomes to other users and advertisers.⁶² This model encourages social media platforms to maximise user engagement by prioritising content that generates high interaction rates, whether this content is true or false.

This is evident in the post-truth era, where social media plays a significant role in diminishing the role of factual information in shaping public opinion.⁶³ The term "post-truth" refers to situations where objective facts are less influential in shaping public opinion than appeals to emotion and personal belief.⁶⁴ In this post-truth era, emotional appeal and personal belief take precedence over objective facts.⁶⁵ This shift is driven by the increasing role of social media, where content that evokes strong emotions tends to be more widely shared and engaged with.⁶⁶ Social media algorithms contribute to the creation of echo chambers and filter bubbles, where users are primarily exposed to information that reinforces their existing beliefs. This selective exposure further entrenches misinformation and disinformation.⁶⁷ The post-truth era is also marked by a growing distrust in traditional media and authoritative sources. This scepticism makes it easier for false

⁵⁹ Boyd M and Ellison B, 'Social network sites: definition, history, and scholarship,' 211.

⁶⁰ Bontridder N and Pouillet Y, 'The role of artificial intelligence in disinformation,' e32-4.

⁶¹ Kim S A, 'Social media algorithms: why you see what you see' *Georgetown Law Technology Review*, 2017, 148-[Georgetown Law Technology Review](#) on 28 January 2025.

⁶² Narayanan A, 'Understanding social media recommendation algorithms' *Knight First Amendment Institute*, 2024, 18 -<https://knightcolumbia.org/research> on 24 January 2025.

⁶³ Harsin J, 'Post-truth and critical communication' *Oxford Research Encyclopedia of Communication*, 2018, 7-<http://dx.doi.org/10.1093/acrefore/9780190228613.013.757> on 14 January 2025.

⁶⁴ Harsin J, 'Post-truth and critical communication,' 1.

⁶⁵ Modreanu S, 'The post-truth era?' *Human and Social Studies*, 2017, 7- [Microsoft Word - REV.HSS 13oct-ref.doc](#) on 10 February 2025.

⁶⁶ Harsin J, 'Post-truth and critical communication,' 11.

⁶⁷ Harsin J, 'Post-truth and critical communication,' 6-7.

information to gain traction, as people are more likely to rely on alternative sources that align with their views.

The post-truth era exacerbates societal polarisation by amplifying divisive content. This can increase social tensions and conflicts, as different groups become more entrenched in their respective viewpoints. Disinformation campaigns in the post-truth era can undermine democratic processes by spreading false information influencing public opinion and electoral outcomes. This manipulation of information erodes trust in democratic institutions and the integrity of elections. The prevalence of disinformation makes it difficult for individuals to engage in meaningful public discourse. Constructive dialogue is hindered when falsehoods overshadow facts, leading to intellectual isolation and a breakdown in mutual understanding. This is apparent during the 2017 and 2022 elections.

During the 2017 elections, Cambridge Analytica played a pivotal role in influencing voter behaviour through data-driven strategies.⁶⁸ Cambridge Analytica did this by harvesting unauthorized data from Facebook, which enabled the firm to profile Kenyan voters based on their online behaviour.⁶⁹ This allowed the firm to deliver highly personalized political ads designed to reinforce tribal and ideological biases.⁷⁰ The recommendation algorithms employed by Facebook ensured that users were exposed to content that aligned with their preexisting political views, creating echo chambers where opposing views were filtered out.⁷¹ These echo chambers deepened division by preventing meaningful discourse and reinforcing the biases the voters already had.

A notable example of disinformation during the 2017 elections' unethical campaigning was the dissemination of false narratives about presidential aspirant Raila Odinga. Harris Media LLC, working with Cambridge Analytica, spread disinformation suggesting that Odinga would forcibly

⁶⁸ Centre for Intellectual Property and Information Technology Law (CIPIT), *Biometric technology, elections, and privacy: Investigating privacy implications of biometric voter registration in Kenya's 2017 election process*, 2017, 25.

⁶⁹ Maweu J, ““Fake elections”? Cyber propaganda, disinformation and the 2017 general elections in Kenya’ *Journal of African Media Studies*, 2020, 67 -< <https://www.tandfonline.com.ezproxy.library.strathmore.edu/doi/epdf/10.1080/23743670.2020.1719858?needAccess=true> >-on 21 March 2025.

⁷⁰ Maweu J, ““Fake elections”? Cyber propaganda, disinformation and the 2017 general elections in Kenya,’ 74.

⁷¹ Abbouda E, Ajwang F and Lugano G, ‘Social media and politics as usual? Exploring the role of social media in the 2022 Kenyan presidential election’ *Journal of Eastern African Studies*, 2024, 323-<<https://www.tandfonline.com/doi/epdf/10.1080/17531055.2024.2377403?needAccess=true>>- on 21 March 2025.

displace "whole tribes from their homes".⁷² This narrative was amplified through social media platforms, creating fear and mistrust among voters.

During the 2022 Kenyan elections, political campaigns extensively leveraged social media platforms to disseminate content that played on voters' emotions. AI algorithms were used to analyze voter data and identify emotional triggers that could be exploited in political messaging. This resulted in the widespread dissemination of emotionally charged content that often overshadowed factual information.

Platforms like TikTok and X (formerly Twitter) played crucial roles in these disinformation campaigns. TikTok, known for its short-form videos, became a hotspot for political disinformation.⁷³ Videos containing manipulated content, including deepfakes, were widely shared, creating false narratives about political candidates.⁷⁴ The rapid spread of such manipulated content was facilitated by TikTok's algorithm, which prioritizes engagement and virality, often at the expense of accuracy.⁷⁵

Social media algorithms played a significant role in creating echo chambers during the election. Platforms like Facebook and X used recommendation algorithms to prioritize content that generated high engagement, often sensational and emotionally charged. This led to the amplification of disinformation, as voters were exposed to a narrow range of perspectives that reinforced their existing beliefs. For example, AI-driven recommendation systems would frequently show users content that aligned with their previous interactions, creating a feedback loop that isolated them from diverse viewpoints. This selective exposure further entrenched misinformation and disinformation, making it difficult for voters to access accurate information and engage in informed discussions. Given these significant negative impacts, it is crucial to develop robust strategies to mitigate these effects.

⁷² Feuer W, 'Cambridge Analytica and its role in Kenya's 2017 elections' *CNBC*, 23 March 2018—<https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html> on 20 March 2025.

⁷³ Madung O, *From dance app to political mercenary: How disinformation on TikTok gaslights political tensions in Kenya*, Mozilla Foundation, 2022, 4 -<
https://assets.mofoprod.net/network/documents/From_Dance_App_to_Political_Mercenary.pdf >-on 20 March 2025.

⁷⁴ Agbele F, 'Disinformation and misinformation during Kenya's 2022 election: Implications for voter confidence in the electoral process.' 3-6.

⁷⁵ Madung O, *From dance app to political mercenary: How disinformation on TikTok gaslights political tensions in Kenya*, 8.

While social media algorithms can have negative impacts, such as spreading misinformation, their positive contributions to personalizing voter education, increasing political engagement, and mobilizing voters for rallies have significantly enhanced the democratic process.

Social media platforms, through recommendation algorithms, tailor content to individual voters, ensuring they receive relevant information that helps them make informed decisions. Social media has been particularly impactful in mobilizing voters for rallies.⁷⁶ These algorithms analyze user data to identify individuals likely to be interested in political events and activities. By targeting these users with tailored content, social media platforms can effectively mobilize supporters and encourage participation in rallies and other political events.⁷⁷

Moreover, social media algorithms enhance the effectiveness of political campaigns by facilitating direct communication between politicians and voters. Politicians can use these platforms to share their messages, address concerns, and mobilize supporters for rallies, fostering a closer connection between politicians and their constituents. This direct interaction enhances transparency and trust, crucial for democratic engagement.

Overall, social media algorithms have revolutionized the way political campaigns mobilize voters for rallies in Kenya. They enhance voter engagement, facilitate direct communication, and ensure that information about political events is disseminated quickly and efficiently. However, despite these positives, the effects of disinformation are profoundly negative. In Kenya's election history, disinformation has often led to significant social and political unrest, undermining the democratic process and exacerbating tensions. The negative impacts of disinformation can outweigh the benefits, highlighting the need for robust measures to mitigate these effects.

Understanding the propagation of information on social media is crucial to grasping its impact. There are three fundamental ways in which the information-propagation component of a platform can be designed: subscription, network and algorithm. In the subscription model, users subscribe to a set of creators, and their feed consists of posts from these creators.⁷⁸ This model is

⁷⁶Abbouda E, Ajwang F and Lugano G, 'Social media and politics as usual? Exploring the role of social media in the 2022 Kenyan presidential election' 322.

⁷⁷ Abbouda E, Ajwang F and Lugano G, 'Social media and politics as usual? Exploring the role of social media in the 2022 Kenyan presidential election' 322.

⁷⁸ Narayanan A, 'Understanding social media recommendation algorithm,' 9.

straightforward and similar to traditional media, where subscribing to a set of newspapers or news channels determines the content one engages with.

The network model, on the other hand, allows users to see posts created by those they've subscribed to as well as posts that users choose to amplify.⁷⁹ The model relies on social connections between users to propagate information. Platforms such as X formerly known as Twitter, follow this model where users see posts based on what individuals in their social network retweet.

In the algorithmic model, the posts a user sees are those that the algorithm predicts that they are likely to engage with.⁸⁰ This model is driven by the platforms' goal to maximize engagement and often leads to amplification of content that is not necessarily accurate but highly engaging.⁸¹

2.3.1 Social Media Algorithms

Social media algorithms are not neutral tools, they are engineered to maximize user content (often prioritizing sensational, emotional content).⁸² This goal is driven by the attention capture model of monetizing user attention. This business model incentivizes the spread of disinformation, as it tends to attract more clicks and shares than factual content. Narayanan explains that the core of the algorithm is engagement prediction, which often leads to the amplification of content that is not necessarily accurate but highly engaging.⁸³ These algorithms can be broadly categorized into two: recommendation algorithms and generative algorithms.⁸⁴

2.3.1.1 Recommendation Algorithms

Social media companies use recommendation algorithms to sort through vast amounts of content posted in these platforms and present it to users in a manageable, appealing way.⁸⁵ This type of algorithm promotes content based on the user demographic, prior history of engagement on the

⁷⁹ Narayanan A, 'Understanding social media recommendation algorithm,' 10.

⁸⁰ Narayanan A, 'Understanding social media recommendation algorithm,' 10.

⁸¹ Bontridder N and Poulet Y, 'The role of artificial intelligence in disinformation,' e32-6.

⁸² Modreanu S, 'The post-truth era?,' 7.

⁸³ Narayanan A, 'Understanding social media recommendation algorithms,' 7.

⁸⁴ Sun H, 'Regulating algorithmic disinformation', 374.

⁸⁵ Narayanan A, 'Understanding social media recommendation algorithm,' 10.

platform, or the conduct of mutuals on these platforms.⁸⁶ These algorithms are divided into three major categories according to the filtering method: collaborative filtering, content-based filtering and hybrid systems.

1. Collaborative filtering is a technique that identifies the preference of a large group of users and recommends content based on the underlying intuition that if users A and B have similar tastes in a product, then A and B are likely to have similar tastes in other products as well.⁸⁷
2. Content-based filtering focuses on the preferences and history of the individual being targeted, recommending content similar to that in which the user previously demonstrated interest.⁸⁸ For example, if a user has shown interest in an article about machine learning, the algorithm will recommend other articles on related topics.
3. Hybrid Systems use elements of both collaborative and content-based filtering. They use multiple algorithms at the same time and combine their results, or they use one algorithm first and refine the results with another algorithm.⁸⁹

Recommendation algorithms can easily spread and amplify fake news. One way in which they do so is by prioritizing the promotion of content that is aligned with a social media company's platform policy over content that users might be most interested in.⁹⁰ This means that these algorithms promote content that receives a large number of likes and engagement. Take the example of Facebook's algorithm which is designed to recommend content with more engagement and likes.⁹¹ This platform pushes pages with engaging connections onto feeds of users even though users do not follow those pages. This dynamic is exploited by troll farms that create fake news

⁸⁶ Roy D and Dutta M, 'A systematic review and research perspective on recommender systems' *Journal of Big Data*, 2022, 2 —<https://doi.org/10.1186/s40537-022-00592-5> on 24 January 2025.

⁸⁷ Roy D and Dutta M, 'A systematic review and research perspective on recommender systems', 4.

⁸⁸ Roy D and Dutta M, 'A systematic review and research perspective on recommender systems', 3.

⁸⁹ Roy D and Dutta M, 'A systematic review and research perspective on recommender systems', 6.

⁹⁰ Sun H, 'Regulating algorithmic disinformation', 374.

⁹¹ Fernández M, Bellogín A, and Cantador I, 'Analysing the effect of recommendation algorithms on the amplification of misinformation' *arXiv*, 2021, 8-<https://doi.org/10.48550/arXiv.2103.14748> on 24 January 2024.

stories specifically designed to generate engagement so that the algorithm amplifies the content, in turn generating more clicks and thus ad revenue.

Recommendation algorithms amplify disinformation to influence user beliefs by creating echo chambers and filter bubbles.⁹² Echo chambers refer to homogenous information environments resulting from users' own choices to follow like-minded individuals on social media, whereas filter bubbles are similar information environments created surreptitiously by a platform's automated efforts to understand individual user preferences and reflect them in its recommendations.⁹³ Recommendation algorithms can distort the character and form of our social capital, that is, our connections to others and, "the level of trust (and trustworthiness) and the informal rules and common understandings that facilitate communication". Filter bubbles trick us into thinking our social and political 'bubbles' are representative of our opinions and views.⁹⁴

2.3.1.2 Generative Algorithms

Generative algorithms are a type of artificial intelligence that creates new content by learning from existing data. These algorithms can generate text, images, music and other forms of media. They are considered particularly powerful because they don't just recognize patterns as recommendation algorithms do, but they create new, original content that mimics the style and structure of the data they were trained on.⁹⁵ There are three several types of generative algorithms namely Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs) and Transformer-based Models.

Generative Adversarial Networks (GANs) consist of two networks, a generator and a discriminator, that work together in a competitive process.⁹⁶ The generator creates new data, while the discriminator evaluates it against real data. Over time, the generator improves its ability to

⁹²Fernández M, Bellogín A, and Cantador I, 'Analysing the effect of recommendation algorithms on the amplification of misinformation,' 9.

⁹³ Bontridder N and Pouillet Y, 'The role of artificial intelligence in disinformation,' e32-7.

⁹⁴ Ibrahim O, Younis E, Mohamed E, and Ismail W, 'Revisiting recommender systems: An investigative survey' Vol 37 *Neural Computing and Applications* Issue 1, 2025, 2167.

⁹⁵ Sun H, 'Regulating algorithmic disinformation', 377.

⁹⁶Banerjee S, Kharate S, and Parmar G, 'Confronting legal hurdles in the battle against AI-driven deepfake misinformation' Volume 33 *Journal of Computational Analysis and Applications* Issue 4, 2024, 2.

create realistic data that can fool the discriminator. GANs have shown state-of-the-art performance in generating photorealistic images, creating new human poses, and even generating artwork. Bots and cyborgs, which are automated accounts programmed to mimic human behaviour, can use GANs to generate realistic fake profiles on social media, which can then be used to spread disinformation.⁹⁷ Bots can engage in false amplifications by amplifying certain hashtags, accounts, or news stories, helping that topic “trend” on social media.⁹⁸ This can create the illusion of widespread support or opposition, influencing public perception and media coverage.

Deepfakes are also an application of the GANs as they use the generator-discriminator framework to create highly realistic fake videos and images.⁹⁹ The generator produces synthetic media, such as a video of a person, while the discriminator network attempts to distinguish between real and fake media. Through this process, the generator adapts to create convincing deepfakes that can convince the discriminator.

Variational Autoencoders (VAEs) are a type of neural network that learns to encode data into a compressed format and then decode it back into its original form.¹⁰⁰ This process involves compressing information, like a picture, into a simpler form and then recreating it from that form. They are also helpful for cleaning up noisy data, such as removing static from a photo, and for spotting unusual patterns that might indicate something is wrong. One of the more controversial uses of VAEs is in creating deepfakes, which are highly realistic fake videos or images that can make it look like someone is saying or doing something they never did.¹⁰¹ These deepfakes can be used to create sensational stories that grab attention, distract from real issues, or manipulate public opinion, especially during important events like elections.

⁹⁷ Montoro-Montaroso A et al., ‘Fighting disinformation with artificial intelligence: fundamentals, advances and challenges’ *Profesional de la Información*, 2023,6- <https://doi.org/10.3145/epi.2023.may.22> on 24 January 2025.

⁹⁸ Lamo M and Calo R, ‘Regulating bot speech’ *UCLA Law Review*, 2018,4- <https://ssrn.com/abstract=3214572> on 28 January 2025.

⁹⁹ Banerjee S, Kharate S, and Parmar G, ‘Confronting legal hurdles in the battle against AI-driven deepfake misinformation,’ 2.

¹⁰⁰ Lamo M and Calo R, ‘Regulating bot speech,’ 8.

¹⁰¹ Sun H, ‘Regulating algorithmic disinformation,’ 379.

Transformer-based Models are trained on large datasets and can produce coherent and contextually relevant text based on a given prompt.¹⁰² Transformer models like GPT-3 and GPT-4 can write essays, answer questions, and generate code. They are also used in natural language processing tasks such as translation and summarization.¹⁰³

The impact of generative algorithms on disinformation is significant. Generative algorithms can be used to create convincing fake news, deepfakes, and other forms of disinformation, which can mislead the public and undermine trust in media and institutions. For example, deepfake videos can depict politicians making false statements, potentially influencing public opinion and election outcomes. Bots can amplify divisive narratives, creating the illusion of widespread support or opposition and influencing public perception.

2.4 Algorithmic Disinformation and Democracy

Digital governance has become an essential pillar of modern democracy, particularly in the context of combating algorithmic disinformation. Digital technologies have significantly transformed how citizens interact with democratic institutions, necessitating new governance frameworks to ensure the integrity of democratic processes.¹⁰⁴ One critical aspect of digital governance is addressing information asymmetry, where voters lack access to reliable sources of information. This asymmetry can lead to an uneven distribution of accurate information, impairing the ability of citizens to make informed decisions and undermining the democratic process.¹⁰⁵

Algorithmic disinformation poses significant threats to democratic processes by impairing the ability of citizens to make informed decisions. In a democracy, the quality of decision-making is heavily reliant on the availability of accurate and reliable information.¹⁰⁶ Disinformation,

¹⁰²Sengar S, Hasan A, Kumar S, and Carroll F, 'Generative artificial intelligence: a systematic review and applications' *Multimedia Tools and Applications*, 2024, 7- <https://doi.org/10.1007/s11042-024-20016-1> on 26 January 2025.

¹⁰³ Montoro-Montarroso, 'Fighting disinformation with artificial intelligence: fundamentals, advances and challenges,' 8.

¹⁰⁴ Bontridder N and Pouillet Y, 'The role of artificial intelligence in disinformation,' e32-6.

¹⁰⁵ Bontridder N and Pouillet Y, 'The role of artificial intelligence in disinformation,' e32-6.

¹⁰⁶ Christiano T, 'Algorithms, manipulation, and democracy' 52 *Canadian Journal of Philosophy* 1, 2022, 122.

particularly when amplified by social media algorithms, undermines this foundation by spreading false or misleading content that can distort public perception and influence electoral outcomes.

The use of algorithmic tools such as deepfakes poses a significant threat to politics and election due to the ability to create highly convincing fake videos featuring political figures. These manipulated videos can be used to spread false information, influence election outcomes, and tarnish the reputation of politicians.¹⁰⁷ This is because they can depict politicians doing things they never did, leading to public confusion and the spread of misinformation. This can in turn manipulate public opinion. These deepfakes can sway voters' opinions and potentially alter the results of elections.

Furthermore, algorithmic disinformation undermines electoral accountability by amplifying false narratives about candidates or institutions. Sun highlights that recommendation algorithms and generative algorithms, such as those creating deepfakes, can spread disinformation at unprecedented levels, distorting the electoral process.¹⁰⁸ This manipulation of information can lead to a lack of accountability, as voters are misled about the actions and intentions of their representatives.

The democratic theory emphasizes the importance of autonomy, which is the ability of individuals to make their own choices and participate in collective decision-making.¹⁰⁹ Autonomy is a cornerstone of democratic governance, as it ensures that citizens can exercise their rights and responsibilities freely and without undue influence. However, disinformation erodes this autonomy by providing individuals with false information, leading them to make decisions based on inaccuracies rather than facts.¹¹⁰ This manipulation of information compromises the integrity of democratic processes and diminishes the capacity of citizens to make autonomous, informed choices.

Disinformation also impairs the ability of individuals to fully participate in public debate.¹¹¹ A healthy democracy relies on the exchange of diverse viewpoints and the ability of citizens to

¹⁰⁷ Confronting Legal Hurdles in the Battle against AI-Driven Deepfake Misinformation

¹⁰⁸ Sun H, 'Regulating algorithmic disinformation', 380.

¹⁰⁹ Munck G, 'Democratic theory and concept formation: ideals and realistic standards', 157.

¹¹⁰ Olaniran B and Williams I, 'Social media effects: Hijacking democracy and civility in civic engagement,' 89.

¹¹¹ Munck G, 'Democratic theory and concept formation: ideals and realistic standards', 150.

engage in meaningful discussions to find common solutions.¹¹² When disinformation is prevalent, it creates an environment where falsehoods can overshadow facts, making it difficult for individuals to discern the truth and engage in constructive dialogue.¹¹³ This not only stifles public debate but also leads to intellectual isolation,¹¹⁴ where individuals are trapped in echo chambers and filter bubbles that reinforce their existing beliefs without exposure to contrasting viewpoints.

The spread of disinformation through social media algorithms can also have detrimental effects on societal peace and the acceptance of contrasting views.¹¹⁵ Disinformation often exploits societal tensions and amplifies divisive content, which can lead to increased polarization and conflict. In Kenya, for example, disinformation campaigns during elections have been used to incite violence and manipulate public opinion, undermining the democratic process and threatening social cohesion. The ability to accept and engage with contrasting views is essential for a functioning democracy, as it fosters mutual understanding and cooperation among citizens. Disinformation disrupts this process by creating mistrust and hostility, making it difficult for individuals to engage in constructive dialogue and work towards common solutions.

2.5 Conclusion

This chapter has provided a comprehensive overview of the conceptual and theoretical foundations of algorithmic disinformation. By defining key terms such as disinformation and misinformation, and exploring the psychological and societal mechanisms that contribute to their spread, I have highlighted the significant impact these phenomena have on public perception and democratic processes. The role of social media and its algorithms in amplifying disinformation has been critically examined, demonstrating how these platforms prioritize engagement over accuracy, leading to the creation of echo chambers and filter bubbles. Furthermore, the chapter has discussed the implications of algorithms in producing and disseminating disinformation, emphasizing the need for robust strategies to mitigate their effects. Overall, understanding these concepts is crucial

¹¹² Bontridder N and Pouillet Y, 'The role of artificial intelligence in disinformation,' e32-6.

¹¹³ Christiano T, 'Algorithms, manipulation, and democracy,' 116.

¹¹⁴ Berelson B, 'Democratic theory and public opinion,' 318.

¹¹⁵ Bontridder N and Pouillet Y, 'The role of artificial intelligence in disinformation,' e32-6.

for developing effective measures to combat algorithmic disinformation and protect the integrity of democratic institutions.

Looking ahead, the next chapter will explore the legal framework governing misinformation and freedom of expression, analyzing how existing regulations address the challenges posed by algorithmic disinformation. This legal analysis will be informed by the insights presented in this chapter, emphasizing the need for robust policies to counteract the digital manipulation of democratic processes.

CHAPTER 3: LEGAL AND REGULATORY FRAMEWORK GOVERNING DISINFORMATION IN KENYA

3.0 Introduction

Social media algorithms, powered by AI, play a critical role in determining what users see, amplifying certain content while suppressing others. While these systems have improved user engagement, they have also contributed to the mass spread of disinformation. In Kenya, where social media is a source of news and a platform for political discourse, the unregulated nature of the algorithmic content has raised concerns about electoral integrity, hate speech and disinformation campaigns.¹¹⁶ From fake news to deepfakes and misinformation campaigns to coordinated campaigns, social media provides opportunities to both the political actors as well as various stakeholders to drive opinion and manipulate sentiment in favour of specific political agendas. As highlighted in Chapter One, the impact of fake news in the last four elections underscores the need for effective regulation of social media platforms to combat disinformation.

Despite the increasing risk posed by social media algorithms, Kenya's legal and regulatory framework has yet to play catch up and remains insufficient to address the challenges associated with this form of disinformation. Currently, Kenya lacks specific laws that regulate how social media platforms use AI-driven algorithms to promote and spread content. Kenya relies on general provisions including the Computer Misuse and Cybercrimes Act (2018), the Data Protection Act (2019), and the Kenya Information and Communications Act (2013) among others that will be discussed in this Chapter. Recognizing these gaps, the Kenya National Artificial Intelligence (AI) Strategy (Draft, 2025-2030) was created as a governance framework but remains aspirational. The law must catch up with technology to ensure the digital space remains safe and trustworthy for all.

This chapter will examine the inadequacies and inefficiencies in Kenya's legal framework in the regulation of algorithmic disinformation in electoral democracies. It further provides a comparative analysis of jurisdictions with advanced regulatory mechanisms and draws lessons from these jurisdictions.

¹¹⁶ Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya', 203.

3.1 The Legal and Institutional Governing Algorithmic Disinformation in Kenya

3.1.1 Legal Framework in Kenya

Kenya's regulatory approach to algorithmic disinformation in elections is fragmented. There is a combination of cybercrime laws and data protection regulations. Below are the specific regulations.

3.1.1.2 The Constitution of Kenya, 2010

The Constitution of Kenya, 2010, is the supreme law of the land. It contains provisions that may be utilized to counter disinformation, especially within the context of election processes. Article 33 of the Constitution guarantees the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas.¹¹⁷ However, this right is not absolute and is subject to limitations, including the need to respect the rights and reputation of others and to protect national security, public order, public health, and public morals.¹¹⁸ This balance ensures that while individuals have the right to express themselves, they must do so responsibly without spreading false information that could harm others or disrupt public order.

Furthermore, Article 35 of the Constitution protects the right to information held by the state and by another person that is required for the exercise or protection of any right or fundamental freedom.¹¹⁹ This provision underscores the need to access accurate information which allows citizens to make informed political decisions, enhancing democracy. This provision also includes the right to the correction or deletion of untrue or misleading information that affects a person. By guaranteeing access to accurate information and providing mechanisms for correcting false information, the Constitution aims to prevent the spread of disinformation and to protect individuals from its harmful effects. Furthermore, this provision highlights the need for relevant legislation to ensure citizens have access to the truth whilst at the same time condemning algorithmic bias towards sensationalism and lies.

¹¹⁷ Article 33, *Constitution of Kenya* (2010).

¹¹⁸ Article 33, *Constitution of Kenya* (2010).

¹¹⁹ Article 35, *Constitution of Kenya* (2010).

Article 38 of the Constitution provides for political liberties and the right to political democracy including the right to free, fair and credible elections and referendums.¹²⁰ Algorithmic disinformation undermines these political rights by altering political discourses, voters' perceptions, and election results. Those who seek to use fake news to discourage voting, vilify opponents, or sow confusion undermine the fairness of the electoral process. To this end, it demands a complex legal and policy approach, which would both directly punish those who spread fake news and indirectly investigate the ways the digital platforms contribute to the problem through their algorithms.

Overall, through these constitutional provisions, Kenya has already provided a solid foundation with which it can contain fake news during electoral processes. However, these provisions do not directly mention the function of algorithmic amplification as used in the dispersal of fake news. This gap shows that there still is much work to be done as it pertains to legal and regulatory reforms to prevent social media from undermining democracy and elections.

3.1.1.2 The Computer Misuse and Cybercrimes Act, 2018

This Act was enacted to detect, prevent, respond to, investigate and prosecute computer and cybercrimes such as the dissemination of false information. It was enacted at a time when there was a rise in the use of digital space for illicit purposes such as identity theft, cyberbullying, hacking and the sharing of untruths to sway public opinion.

Section 22 of the Act criminalises the *intentional publication* of false, misleading or fictitious data or information with the intent to mislead or deceive the public.¹²¹ This provision was tailored to discourage individuals or groups from allowing such falsehoods to be distributed purposely. It specifically states that any person who publishes false information that is likely to cause panic, chaos, or violence, or that is likely to discredit the reputation of a person, commits an offence.¹²² This provision is crucial in curbing the spread of false information that can have serious societal impacts, such as inciting violence or damaging reputations. This aligns with Article 33 of the Constitution which limits the freedom of expression in the above instances. This provision fails to

¹²⁰ Article 38, *Constitution of Kenya* (2010).

¹²¹ Section 22, *Computer Misuse and Cybercrimes Act* (No.5 of 2018).

¹²² Article 33, *Constitution of Kenya* (2010).

hold social media platforms accountable for amplifying false election information through their algorithms.

Another provision is Section 23 which addresses the use of electronic communication to harass, intimidate, or cause substantial emotional distress to a person.¹²³ During elections, political opponents are bombarded with fake news which may contain defamation information, fake images and even threats. It is for this reason that the incorporation of cyber harassment as included in the Act is a positive step in endeavouring to shield individuals from such abuse. This section includes provisions to combat the spread of false information intended to harass or intimidate individuals such as political candidates and voters. This provision however lacks provisions targeting algorithm disinformation or content curation that could cause cyber harassment. The enforcement of this provision would be difficult as it is hard to ascertain the culprit especially if such harassment is driven by algorithms.

The enactment of the CMCA also led to the creation of the National Computer and Cybercrimes Coordination Committee, a body tasked with overseeing cybersecurity regulations. Its role in curbing algorithmic disinformation remains limited due to inadequate legal provisions and enforcement mechanisms. Seeing how much social media algorithms play a role in forming political discourse, there is more to be done to update the law regarding individuals and the platforms themselves as major actors of electoral interference and disinformation.

3.1.1.3 The Data Protection Act, 2019

The Data Protection Act, of 2019, was enacted to provide guidelines on the processing of personal data and to protect individuals' privacy. This Act gives effect to Article 31(c) and (d) of the Constitution of Kenya, which guarantees the right to privacy. The Act establishes the Office of the Data Protection Commissioner, which is responsible for overseeing the implementation of the Act and ensuring compliance with its provisions.

Section 25 of the Act outlines the legal requirements for processing personal data, emphasizing that data should be collected for clear, specific, and lawful purposes and must not be used in a way

¹²³ Section 23, *Computer Misuse and Cybercrimes Act* (No.5 of 2018).

that conflicts with those purposes.¹²⁴ This provision aims to ensure that personal data is not used to create or spread false information. This provision, however, does not mandate social media platforms to disclose how user data is utilized for algorithmic recommendations that may influence election-related narratives.

The Act grants data subjects various rights, including access to their personal data, the ability to correct or delete inaccurate information, and the right to object to its processing.¹²⁵ These rights empower individuals to take control of their personal data and to prevent its misuse for disinformation purposes.

3.1.1.4 The Elections Act, 2011

The Elections Act is one of the legal frameworks that guide electoral processes in Kenya and includes measures to prevent the use of disinformation during campaigns. Section 67 is one of the most direct provisions as it makes it unlawful to make a false statement with the intent of influencing an election result.¹²⁶ This section was designed to protect the electoral processes by denying those bent on using falsehood to negatively influence an opponent, voters or the public at large an opportunity to do so. In so doing, the Act supports the constitutional provisions regarding freedom of political association and the holding of free and fair elections.¹²⁷

However, the Elections Act focuses on the direct transmission of falsehoods by a person and does not consider the role of amplification of electoral disinformation. Social media uses algorithms that favour engagement, which results in the promotion of sensational and misleading electoral information. This algorithmic bias helps in the expedited and extensive dissemination of fake news, which may sometimes spread outside the control of the source. The issue of algorithmic amplification has not been addressed in the Elections Act, essentially leaving the law deprived of regulation to combat disinformation in digital environments beyond the actions of tech platforms.

¹²⁴ Section 25, *Data Protection Act* (No.24 of 2019).

¹²⁵ Section 26, *Data Protection Act* (No.24 of 2019).

¹²⁶ Section 67, *Elections Act* (No.24 of 2011).

¹²⁷ Article 81, *Constitution of Kenya* (2010).

3.1.1.5 *National Cohesion and Integration Act, 2008*

The National Cohesion and Integration Act was established to foster unity and integration by prohibiting ethnic-based discrimination and criminalizing hate speech and incitement. This legislation is particularly significant in addressing algorithmic disinformation, which can heighten ethnic tensions, especially during elections. Section 13 of the Act restricts the use of threatening, abusive, or offensive language or behavior intended to incite ethnic hostility. This provision plays a key role in limiting the spread of inflammatory content that could lead to violence and disrupt social stability.

A major challenge, however, is that the Act primarily targets explicit hate speech and ethnic incitement without directly addressing how social media algorithms contribute to amplifying such content. These algorithms often prioritize engagement, which can lead to the promotion of sensational and divisive material, exacerbating ethnic tensions. As a result, harmful content spreads rapidly, making it increasingly difficult for the NCIC to monitor and regulate.

3.1.2 Institutional Framework in Kenya

3.1.2.1 *National Cohesion and Integration Commission(NCIC)*

The National Cohesion and Integration Commission (NCIC) was established under the National Cohesion and Integration Act (2008) to promote national unity and integration by addressing and reducing inter-ethnic conflicts.¹²⁸ The NCIC has the authority to summon witnesses, conduct investigations, and issue compliance notices to ensure adherence to the Act's provisions.¹²⁹ Section 62 of the Act further empowers the NCIC to monitor and address the spread of disinformation that targets ethnic groups.¹³⁰ The Commission plays a vital role in ensuring that social media platforms and other digital spaces do not become breeding grounds for ethnic hatred and division.¹³¹

Despite its critical mandate, the NCIC faces significant challenges in regulating digital platforms. The Commission lacks the technical capacity to monitor and control the spread of disinformation

¹²⁸Section 15, *National Cohesion and Integration Act* (No.12 of 2008).

¹²⁹ Section 15, *National Cohesion and Integration Act* (No.12 of 2008).

¹³⁰Section 62, *National Cohesion and Integration Act* ((No.12 of 2008).

¹³¹ Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya', 234.

on social media, where algorithms can amplify hate speech and ethnic incitement. This limitation hinders the NCIC's ability to effectively address the rapid dissemination of inflammatory content online.

3.1.2.2 Independent Electoral and Boundaries Commission(IEBC)

The Independent Electoral and Boundaries Commission (IEBC) is a regulatory body established under the Constitution of Kenya and the Independent Electoral and Boundaries Commission Act. Its mandate includes overseeing and managing elections and referendums for all elective positions outlined in the Constitution.¹³²Its mandate includes the continuous registration of voters, delimitation of constituencies and wards, regulation of political parties, settlement of electoral disputes, and voter education.¹³³

Despite its comprehensive mandate, the IEBC has faced significant challenges in regulating algorithmic disinformation, particularly during the 2022 general elections. Disinformation campaigns on platforms significantly influenced public opinion and voter behaviour. The IEBC's failure to effectively counter these digital disinformation efforts highlighted its limited capacity to address the complexities of algorithmic amplification of false information.

3.1.2.3 Communications Authority of Kenya(CAK)

The Communications Authority of Kenya (CAK), formed under the Kenya Information and Communications Act (KICA) of 1998, serves as the independent regulatory body for Kenya's ICT sector. The CAK's responsibilities encompass the regulation of telecommunications, e-commerce, broadcasting, cybersecurity, and postal and courier services..¹³⁴ The CAK is responsible for licensing communication systems and services, overseeing the allocation of frequency spectrum and numbering resources, promoting e-commerce growth, and safeguarding consumer rights within the communications sector. However, it encounters challenges in addressing algorithmic disinformation. A key limitation in its regulatory framework is the lack of sufficient technical

¹³² Article 88, *Constitution of Kenya* (2010).

¹³³ Section 4, *Independent Electoral and Boundaries Commission Act* (No.9 of 2011).

¹³⁴ Section 5A, *Kenya Information and Communications (Amendment) Act* (No. 41A of 2013).

expertise to assess and oversee the algorithms used by social media platforms for content curation and recommendation.

3.2 The Inadequacies of the Legal Framework on Algorithmic Disinformation

Although Kenya has a variety of laws that outlaw disinformation to a certain extent, there is still a lack of legislation specifically targeting algorithmic disinformation. While existing legislation has regarded the deliberate spread of fake news(disinformation), incitement, and cyberbullying as criminal acts, there are still no binding regulations for social media algorithms. The current laws fail to regulate the role of algorithms in amplifying falsehoods, leaving loopholes that allow for the unchecked spread of disinformation. The following gaps exist:

3.2.1 Absence of a legal definition of algorithmic disinformation

Currently, Kenyan laws broadly address disinformation but they do not specifically define algorithmically amplified disinformation. This lack of specificity makes it challenging to regulate AI-driven misinformation campaigns effectively. Sun defines Algorithmic disinformation as the use of algorithms to intentionally amplify and spread false or misleading information.¹³⁵ Without a clear legal definition, it is difficult to distinguish between traditional disinformation and algorithm-driven disinformation.

The CMCA criminalizes the intentional publication of false information but does not differentiate between human-generated and AI-generated content. Similarly, the DPA focuses on the lawful processing of personal data but does not mandate transparency in how social media platforms use algorithms to recommend content.

To address this gap, it is essential to propose the inclusion of a statutory definition of algorithmic disinformation in electoral laws. This definition should distinguish between different types of disinformation, including organic disinformation (false information spread by individuals)and algorithmically boosted propaganda (content amplified by social media algorithms). By clearly defining these categories, the legal framework can better target and regulate the specific mechanisms through which disinformation spreads.

¹³⁵ Sun H, 'Regulating algorithmic disinformation,' 373.

3.2.2 No Specific Regulation for Social Media Algorithms in Political Content Moderation

Another critical gap in Kenya's legal and regulatory framework is the lack of specific regulation for social media algorithms in political content moderation. While existing laws address false information, they do not impose any obligations on social media platforms regarding algorithmic transparency in political content. This gap allows platforms to algorithmically amplify false and misleading content for engagement, worsening electoral disinformation.

Social media algorithms significantly influence the information presented to users. These algorithms tend to prioritize content that garners high engagement, often highlighting sensational and polarizing material. This can shape public opinion and voter behavior. During elections, such algorithms can facilitate the spread of false or misleading information, potentially compromising the integrity of the electoral process.

3.2.3. Lack of Regulations Governing Electoral Algorithmic Disinformation

The Elections Act (2011) primarily focuses on traditional campaign activities and does not address the complexities of AI-powered voter manipulation through micro-targeting. Political microtargeting involves using data analytics and AI to deliver personalized political messages to specific segments of the electorate based on their demographic, psychographic, and behavioural data.¹³⁶ This technique can significantly influence voter behaviour by tailoring messages to resonate with individuals' unique preferences and vulnerabilities.

During Kenya's 2017 and 2022 elections, there were notable instances of microtargeted disinformation campaigns influenced by foreign entities, such as Cambridge Analytica.¹³⁷ These campaigns exploited personal data to create highly targeted and persuasive political ads that manipulated voter perceptions and decisions. The lack of specific regulations governing the use of algorithms and data analytics in political advertising has allowed such practices to proliferate without adequate oversight.

The current legal framework does not require political advertisers to disclose the data sources used in ad targeting or to label AI-generated or deepfake content. This lack of transparency makes it

¹³⁶ Roy D and Dutta M, 'A systematic review and research perspective on recommender systems,' 2.

¹³⁷ Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya', 212.

difficult for voters to discern the authenticity of political messages and to understand how their data is being used to influence their voting behaviour.

3.2.4 No Platform Liability for Algorithmic Disinformation

The existing laws focus on the individual as the perpetrator of disinformation. For example, the Computer Misuse and Cybercrimes Act (2018), criminalize individuals who spread false information but do not hold social media platforms accountable for amplifying such content through their algorithms.¹³⁸ This lack of accountability allows platforms to prioritize engagement over accuracy, leading to the widespread dissemination of sensational and misleading information.

3.2.5 Lack of Coordinated Regulation

Currently CAK, NCIC, and IEBC operate on their own, each with its mandate and regulatory scope. This fragmented approach has led to enforcement failures and inefficiencies in addressing the complex and evolving nature of digital disinformation.

The CAK is responsible for regulating the ICT industry, including telecommunications, e-commerce, broadcasting, and cybersecurity. However, its focus is primarily on technical and infrastructural aspects. The NCIC, on the other hand, is tasked with promoting national cohesion and addressing ethnic discrimination and hate speech. While it plays a crucial role in monitoring and investigating complaints of ethnic incitement, it does not have the technical expertise or authority to regulate digital platforms and their algorithms. IEBC is responsible for overseeing the conduct of elections and referendums, including voter registration, delimitation of constituencies, and voter education. Despite its comprehensive mandate, the IEBC has struggled to address the spread of digital disinformation during elections, as it lacks the technical resources and expertise to monitor and counter algorithmic amplification of false information.

The absence of a single body responsible for digital election integrity has resulted in a lack of coordinated efforts to combat algorithmic disinformation. Each agency operates within its regulatory framework, leading to gaps in oversight and enforcement.

¹³⁸ Section 22, *Computer Misuse and Cybercrimes Act* (No.5 of 2018).

3.3 Legislative Attempts and Their Failures

Kenya has made several attempts to regulate social media and curb the spread of disinformation through legislative means. One notable effort was *The Kenya Information and Communication (Amendment) Bill, 2019*, “Social Media Bill.” This Bill sought to introduce legal obligations for social media users and administrators to control the spread of false information online. Despite passing the first reading in Parliament, it failed to progress further due to concerns over its broad regulatory scope and potential infringement on fundamental rights, particularly freedom of expression.

The Bill proposed measures such as mandatory registration for users with more than 5,000 followers,¹³⁹ licensing requirements for social media group administrators,¹⁴⁰ and penalties for publishing false information.¹⁴¹ While these provisions aimed to enhance accountability, they overlooked a critical aspect of digital disinformation—the role of social media algorithms in amplifying electoral falsehoods. By focusing primarily on individual users rather than the platforms themselves, the Bill failed to address how algorithmic systems manipulate the visibility of political content, favouring engagement-driven sensationalism over factual accuracy. The Bill lacked mechanisms to ensure platform accountability for algorithmic bias in content recommendation. The absence of clear guidelines on content moderation and enforcement also contributed to its rejection, as concerns arose over the arbitrary application and the difficulty of defining false information in political contexts.

The failure of the Social Media Bill underscores the need for a more comprehensive regulatory framework that directly addresses algorithmic disinformation in electoral democracy. Future legislative efforts should focus on platform transparency, compelling social media companies to disclose how their recommendation systems influence the spread of election-related content. Learning from global best practices can help Kenya design more effective policies that ensure fair electoral processes without infringing on democratic freedoms.

¹³⁹ Section 84IA(2)(b), *The Kenya Information and Communications (Amendment) Bill* (Bill No. 61 of 2019).

¹⁴⁰ Section 84IC(2), *The Kenya Information and Communications (Amendment) Bill* (Bill No. 61 of 2019).

¹⁴¹ Section 84IC(3), *The Kenya Information and Communications (Amendment) Bill* (Bill No. 61 of 2019).

3.4 Comparative Analysis

In this section, I will explore the legal and regulatory frameworks of the European Union(EU)to address the gaps identified in Kenya’s approach to algorithmic disinformation.

3.4.1 Overview of the Existing Laws

The European Union has developed a comprehensive legal and regulatory framework to address online disinformation.¹⁴² The EU’s Digital Service Act(2022), Political Advertising Regulations(2023) and AI Act provide a framework for holding social media platforms accountable ensuring transparency in algorithmic content curation. Unlike Kenya’s fragmented laws, the EU has developed comprehensive legal obligations that impose transparency, liability, and enforcement measures on digital service providers

The Digital Services Act(DSA) is a landmark legislation formulated to create a safer and more predictable digital environment. It does this by imposing stringent requirements on online platforms operating in the EU. Article 15 mandates that providers of intermediary services publish annual reports on their content moderation activities, including information on orders from authorities, notices submitted, and the use of automated tools. Article 24 builds on these transparency requirements and imposes additional obligations on providers of online platforms, such as reporting on dispute settlements, suspensions, and active recipients. Article 26 requires online platforms to assess the extent to which their algorithms contribute to the spread of disinformation, particularly in political contexts, while Article 42 mandates that large social media platforms disclose how their recommendation systems prioritize election-related content.

The DSA creates the European Board for Digital Services, which oversees the implementation and enforcement of the regulation.¹⁴³ National Digital Services Coordinators in each EU member state are responsible for monitoring compliance and coordinating with the European Commission.

The AI Act, on the other hand, creates a framework for AI governance, emphasising transparency, accountability, and safety in the deployment of AI systems. Article 13 of this Act provides that developers and deployers of AI systems must conduct impact assessments, ensure fairness and

¹⁴² Bontridder N and Poulet Y, ‘The role of artificial intelligence in disinformation,’e32-12.

¹⁴³ Article 50, *Digital Services Act*, 19 October 2022, Directive 2000/31/EC.

non-discrimination, and provide clear explanations of how their AI systems function. This includes disclosing the data sources and algorithms used in AI-driven content moderation and political advertising.

The Political Advertising Regulation aims to enhance transparency and accountability in political advertising, particularly in the context of elections and referendums. This regulation addresses concerns about information manipulation and foreign interference in electoral processes. It requires transparency labels to be made available for political advertisements. As per Article 7, these labels must identify political advertisements as such and provide key information, including the sponsor, the election or referendum to which they are linked, the amounts paid, and any use of targeting techniques.

3.4.2 Comparison with Kenya's Regulatory System

With regard to the classification of algorithmic disinformation, the Computer Misuse and Cybercrimes Act (2018) criminalizes the publication of false information under Section 22 but does not distinguish between disinformation spread by human actors and disinformation amplified by AI-driven algorithms. This lack of a precise legal definition makes it challenging to address automated disinformation. In the EU, the DSA explicitly recognizes the systemic risks posed by AI-powered disinformation. Articles 26 and 42 require platforms to assess and disclose how their algorithms contribute to the spread of disinformation, particularly in political contexts.

In Kenya, the legal framework holds individuals accountable for spreading false information but does not impose liability on social media platforms that amplify disinformation through algorithms. The CMCA (Section 23) penalizes those who intentionally distribute misleading content but does not require platforms to mitigate algorithmic disinformation. In the EU, the DSA directly regulates platform accountability. Articles 27, 33, and 41 impose due diligence obligations, mandate independent algorithmic audits, and impose significant fines for non-compliance. This ensures that platforms are held accountable for their role in spreading disinformation and are required to take proactive measures to mitigate these risks.

Furthermore, with regard to transparency and reporting, there are no specific requirements for platforms to publish transparency reports on their content moderation activities or the use of

automated tools in Kenya. On the other hand, articles 15 and 24 of the DSA require platforms to publish detailed transparency reports, including information on content moderation, dispute settlements, and the use of automated tools. This enhances regulatory oversight and accountability by ensuring that platforms disclose detailed information about their content moderation practices, user engagement, and interactions with regulatory authorities.

As for institutional mandate, in Kenya, the regulatory landscape is fragmented, with different agencies—including the Communications Authority of Kenya (CAK), the National Cohesion and Integration Commission (NCIC), and the Independent Electoral and Boundaries Commission (IEBC)—working in isolation to address disinformation. In the EU, the DSA establishes a centralized model for enforcement. The European Board for Digital Services (EBDS) oversees the implementation of disinformation policies across EU member states, while National Digital Services Coordinators (DSCs) ensure platform compliance with transparency and content moderation requirements. This centralized approach ensures consistent enforcement and coordination across member states.

3.5 Conclusion

This chapter has highlighted the significant gaps in Kenya's legal and regulatory framework in addressing algorithmic disinformation, particularly during elections. Despite existing laws like the Constitution, the Computer Misuse and Cybercrimes Act, and the Data Protection Act, there is a lack of specific regulations targeting the role of social media algorithms in spreading false information. The fragmented regulatory approach further complicates enforcement. By drawing lessons from the European Union's comprehensive framework, Kenya can enhance its regulations to ensure transparency, accountability, and platform liability, thereby protecting electoral integrity and democracy from the threats posed by algorithmic disinformation.

CHAPTER 4: RECOMMENDATIONS

4.0 Introduction

This chapter presents a series of recommendations aimed at strengthening Kenya's legal and regulatory framework to effectively combat algorithmic disinformation. Drawing lessons from the European Union's advanced regulatory mechanisms, including the Digital Services Act, the AI Act, and the Political Advertising Regulations, these recommendations propose measures to enhance transparency, accountability, and platform liability. The goal is to address the current gaps in Kenya's approach to regulating social media algorithms and to protect the integrity of electoral processes and democracy from the threats posed by disinformation.

4.1 Defining Algorithmic Disinformation

Kenya's legal framework must include a clear and precise definition of algorithmic disinformation. This definition should distinguish between organic disinformation and algorithmic disinformation. Organic disinformation typically originates from individuals or groups who intentionally spread false information. This can include misleading news articles, doctored images, or false claims shared on social media platforms. On the other hand, algorithmically amplified disinformation refers to information artificially boosted by social media algorithms, often without the user's knowledge. These algorithms prioritise and recommend content based on various factors, such as engagement, user preferences, and advertising revenue, which can inadvertently amplify false or misleading information.

This definition should be incorporated through the amendment of the Computer Misuse and Cybercrimes Act. By amending this act to include specific provisions for algorithmic disinformation, Kenya can better address the unique challenges posed by the amplification of false information through social media algorithms. Alternatively, a new legislative framework addressing digital disinformation could be established, modelled after international best practices.

A comparative approach can strengthen this definition. The European Union's DSA provides a structured approach to defining and addressing disinformation, particularly in the context of algorithmic amplification. While the DSA does not explicitly define "algorithmic disinformation" as a standalone term, it categorizes disinformation as systemic risks that arise when false or misleading content is disseminated in a way that threatens democratic processes, public security,

or fundamental rights.¹⁴⁴ By framing disinformation as a systemic risk rather than just an individual act, the DSA ensures that enforcement mechanisms can target both content creators and the platforms that algorithmically amplify such content.

By defining disinformation in terms of systemic risks and algorithmic amplification the DSA makes it significantly easier to identify responsible parties. This structured approach enables regulators to trace how disinformation originates, how it is algorithmically distributed, and who benefits from its dissemination, thereby ensuring more effective enforcement.

4.2 Regulating Social Media Algorithms

Kenya must implement specific regulations governing social media algorithms, particularly in the context of political content moderation. These regulations should mandate transparency in how algorithms prioritize and recommend content. The regulations should include provisions for conducting algorithmic audits. These audits should assess the extent to which social media algorithms contribute to the spread of disinformation. They can identify potential biases within the algorithms and recommend measures to mitigate their impact. For example, if an audit reveals that an algorithm disproportionately promotes sensational or misleading content, the platform should be required to adjust the algorithm to prioritize more accurate and reliable information.

To ensure the effectiveness of these audits, it is crucial to detail the process by which they will be conducted. These audits should assess whether algorithms disproportionately amplify misleading or politically skewed content, whether coordinated disinformation exploits platform ranking systems, and evaluate compliance with regulatory standards. An independent body could be tasked with carrying out these audits. Establishing a dedicated regulatory body with the mandate to oversee algorithmic audits would provide a structured approach to this process.

Given Kenya's limited technical capacity, as noted in Chapter 3, discussing funding or international partnerships could enhance the feasibility of these audits. International organizations such as UNESCO's Information for All Programme (IFAP), the European Commission's AI and Disinformation Taskforce, and African Union-backed digital governance initiatives could provide training programs for Kenyan regulators, technical assistance, funding, and expertise to support Kenya in conducting thorough algorithmic audits. These partnerships could also facilitate

¹⁴⁴ Article 3(1)(j) *Digital Services Act*, 19 October 2022, Directive 2000/31/EC.

knowledge exchange and capacity building, enabling Kenyan regulators to develop the necessary skills and infrastructure to effectively monitor and audit social media algorithms.

Furthermore, establishing clear guidelines and standards for algorithmic audits is essential. These guidelines should outline the objectives, methodologies, and reporting requirements for the audits. Regular audits should be conducted to ensure ongoing compliance and to address any emerging issues related to algorithmic disinformation. Audit findings should be made publicly available to promote accountability and trust.

4.3 Creating a Centralized Body

Kenya should establish a centralized body responsible for digital election integrity. This body should have a clear mandate to coordinate efforts among existing agencies and ensure a unified approach to combating algorithmic disinformation. The centralized body should work closely with the CAK, NCIC, IEBC to develop and implement comprehensive regulations that address the specific challenges posed by algorithmic disinformation.

The structure of this centralized body is crucial for its effectiveness. One option is to establish a Digital Election Integrity Commission (DEIC) as an independent regulatory agency tasked exclusively with overseeing digital political content. Alternatively, this mandate could be incorporated within an existing institution, such as the IEBC, expanding its responsibilities beyond traditional election management to include monitoring, auditing, and enforcing regulations on digital disinformation. However, extending the mandate of an existing body like the IEBC could leverage existing infrastructure and resources, potentially reducing the costs and complexities associated with establishing a new entity.

One of the key functions of the centralized body should be to facilitate information sharing and collaboration among regulatory agencies. By creating a platform for regular communication and coordination, the centralized body can ensure that all relevant agencies are aware of the latest developments in digital disinformation and can respond effectively. This can help to prevent gaps in oversight and enforcement and ensure a more cohesive regulatory approach.

Potential challenges in establishing this centralized body must be addressed to ensure its success. Political interference is a significant concern, given Kenya's history of electoral disputes. Ensuring the independence and impartiality of the centralized body is essential to maintaining public trust

and credibility. If placed under an existing agency, safeguards must be put in place to ensure non-partisan oversight, such as requiring multi-stakeholder representation, including civil society, academia, and the private sector. This can be achieved through legal safeguards that protect the body from undue political influence and ensure transparent and accountable operations.

Funding is another critical challenge. Establishing and maintaining a centralized body for digital election integrity requires substantial financial resources. Discussing potential funding sources, such as government allocations, international grants, and partnerships with organizations like UNESCO, can enhance the feasibility of this initiative. International partnerships can provide technical assistance, funding, and expertise, helping Kenya build the necessary capacity to effectively combat algorithmic disinformation.

Comparative models provide valuable insights into how such a body could function. The European Union's DSCs established under the DSA, serve as independent national regulators overseeing platform accountability and algorithmic transparency. Adopting a hybrid approach that combines strong regulatory powers with independent oversight mechanisms would help ensure Kenya's centralized body remains effective, transparent, and resilient to political influence. By creating a centralized, well-funded, and politically independent body, Kenya can significantly enhance its ability to monitor and mitigate algorithmic disinformation, ensuring fairer electoral processes and protecting the integrity of democratic discourse.

4.4 Transparency and Reporting Requirements

Transparency reports should provide detailed information on how social media algorithms prioritize and recommend content. This includes disclosing the criteria and data sources used by the algorithms, as well as any changes made to the algorithms over time. By making this information publicly available, regulators and the public can better understand the role of algorithms in spreading disinformation and hold platforms accountable for their actions.

In addition to algorithmic transparency, transparency reports should also include information on content moderation practices. This includes data on the number of content removal requests received and processed, the types of content removed, and the reasons for removal. By providing this information, social media platforms can demonstrate their commitment to combating disinformation and ensure that their content moderation practices are fair and consistent.

4.5 Conclusion

Strengthening Kenya's response to algorithmic disinformation requires a comprehensive legal and regulatory framework that ensures transparency, accountability, and platform responsibility. By defining algorithmic disinformation within the CMCA , Kenya can create a clear legal basis for addressing the spread of misleading content through social media algorithms. Implementing mandatory algorithmic audits, establishing a centralized body for digital election integrity, and enforcing transparency and reporting requirements for social media platforms will enhance oversight and mitigate the risks posed by disinformation. Through strong legal safeguards, independent oversight, and international collaboration, Kenya can build a resilient system that combats algorithmic disinformation while promoting fairness and integrity in electoral processes.

CHAPTER 5: CONCLUSION

This study highlights the crucial role social media algorithms play in shaping political discourse and electoral integrity. Algorithmic disinformation is a growing challenge for democracies, especially in Kenya, where elections have been historically susceptible to manipulation through misinformation and disinformation. This research aims to bridge the gap between the legal framework governing disinformation and the realities of algorithmic amplification, showing the shortcomings of Kenya's current regulatory mechanisms and proposing reforms.

By examining Kenya's legal landscape, the study reveals significant gaps in addressing disinformation, particularly that amplified by social media algorithms. The lack of a clear legal definition of algorithmic disinformation, the absence of platform liability, and an uncoordinated regulatory approach contribute to the persistence of disinformation as a threat to electoral democracy. Comparative analysis of regulatory approaches, especially from the European Union, provides valuable insights into strengthening Kenya's regulatory framework.

One of the key theoretical foundations of this research was the democratic theory which emphasises transparency, accountability, and citizen participation is a key foundation of this research. Access to accurate information is fundamental for informed decision-making by citizens. However, algorithmic disinformation distorts public discourse, manipulates voter perceptions, and undermines these democratic ideals. The study's recommendations advocate for stronger regulatory oversight, increased transparency from digital platforms, and greater public awareness of algorithmic influences on political content. The marketplace of ideas theory that free and open discourse allows the best ideas to prevail, is also challenged by algorithmic content curation. Algorithms prioritize engagement over accuracy, creating echo chambers that reinforce biases rather than fostering a balanced exchange of ideas. This study's recommendations such as algorithmic audits and increased transparency in content moderation aim to restore balance in the digital marketplace of ideas by ensuring disinformation is not disproportionately amplified over factual content.

A significant contribution of this study is framing algorithmic disinformation as a systemic risk rather than an isolated phenomenon. Kenya's recent electoral history shows that disinformation campaigns are often highly coordinated and strategically disseminated to achieve political objectives. The recommendation to establish a centralized regulatory body dedicated to digital

election integrity reflects the need for a coordinated and comprehensive approach to mitigating the impact of algorithmic disinformation.

This study also addresses the research gap on platform accountability in Kenya. Existing legislation, such as the CMCA criminalize false information but do not impose direct obligations on social media platforms to mitigate the amplification of disinformation. By advocating for platform liability and transparency requirements, this study contributes to the growing discourse on the role of technology companies in safeguarding democratic integrity.

Integrating international best practices enhances the study's contribution to policy development. Lessons from the European Union offer a structured approach to addressing algorithmic disinformation in Kenya. Proposals for mandatory algorithmic audits, transparency reports, and clear accountability mechanisms align with global trends in digital governance, positioning Kenya as a potential leader in regulating social media in electoral contexts.

In conclusion, while algorithmic disinformation poses a formidable threat to electoral integrity in Kenya, targeted legal and policy reforms can mitigate its impact. By linking recommendations to democratic and marketplace of ideas theories, the study reinforces the importance of regulatory interventions in protecting free and fair elections. Proposed measures ranging from algorithmic transparency to establishing a centralized regulatory body aim to create a more accountable digital ecosystem that upholds democratic values of truth, fairness, and informed decision-making. Despite challenges in enforcing compliance among global technology giants, the study offers a roadmap for strengthening Kenya's resilience against digital electoral manipulation. This research contributes to filling the legal and policy gap on algorithmic disinformation in Kenya, providing a foundation for further academic inquiry and legislative action.

BIBLIOGRAPHY

Books

Mill JS, *On Liberty*, Hackett Publishing, Indianapolis, 1978.

Chapters in Books

Olaniran B and Williams I, 'Social media effects: Hijacking democracy and civility in civic engagement' in *Platforms, Protests, and the Challenge of Networked Democracy*, 2020, 78-89.

Hard Copy Journals

Margetts H, 'Rethinking democracy with social media' 90 *The Political Quarterly* S1, 2018.

Rutenburg I and Sugow A, 'Regulation of the social media in electoral democracies: A case of Kenya' Vol VII(I) *SOAS Law Journal*, 2020.

Ikran A, 'Exploring co-regulation as a solution to automated disinformation in Kenya' 3 *Journal of Intellectual Property and Information Technology Law* 1, 2023.

Boyd M and Ellison B, 'Social network sites: definition, history, and scholarship' 13 *Journal of Computer-Mediated Communication* 1, 2007.

Ibrahim O, Younis E, Mohamed E , and Ismail W, 'Revisiting recommender systems: An investigative survey' 37 *Neural Computing and Applications* 1, 2025

Banerjee S, Kharate S, and Parmar G, 'Confronting legal hurdles in the battle against AI-driven deepfake misinformation' 33 *Journal of Computational Analysis and Applications* 4, 2024.

Christiano T, 'Algorithms, manipulation, and democracy' 52 *Canadian Journal of Philosophy* 1, 2022.

Online Journal Articles

Bontridder N and Poulet Y, 'The role of artificial intelligence in disinformation' *Data & Policy*, 2021.

Chalke S and Mishra D, 'Studying the impact of social media algorithms on the spread of misinformation and its effects on society' *International Journal of Advanced Research in Science Communication and Technology*, 2023.

Sugow A, 'The right to be wrong: Examining the (Im)possibilities of regulating fake news while preserving the freedom of expression in Kenya' *Strathmore Law Review*, 2019.

Sun H, 'Regulating algorithmic disinformation' *The Columbia Journal of Law & The Arts*, 2013.

Agbele F, 'Disinformation and misinformation during Kenya's 2022 election: Implications for voter confidence in the electoral process' *MegaTrends Afrika*, 2023.

Mudavadi K, Matanji F, Diop L, Tully M and Madrid-Morales D, 'Stakeholder perceptions of regulatory responses to misinformation in Kenya and Senegal' *Sage Journals*, 2024.

Munck G, 'Democratic theory and concept formation: ideals and realistic standards', 2023.

Bobbio L, 'Designing effective public participation' *Policy and Society*, 2019.

Berelson B, 'Democratic theory and public opinion' *The Public Opinion Quarterly*, 1952.

Ziemer C-T and Rothmund T, 'Psychological underpinnings of misinformation countermeasures: A systematic scoping review' *Journal of Media Psychology: Theories, Methods, and Applications*, 2024.

Heitmayer M, 'The second wave of attention economics: Attention as a universal symbolic currency on social media and beyond' *Interacting with Computers*, 2024.

Kaplan A and Haenlein M, 'Users of the world, unite! The challenges and opportunities of social media' *Business Horizons*, 2010.

Kim S A, 'Social media algorithms: why you see what you see' *Georgetown Law Technology Review*, 2017.

Narayanan A, 'Understanding social media recommendation algorithms' *Knight First Amendment Institute*, 2024.

Harsin J, 'Post-truth and critical communication' *Oxford Research Encyclopedia of Communication*, 2018.

Abbouda E, Ajwang F and Lugano G, 'Social media and politics as usual? Exploring the role of social media in the 2022 Kenyan presidential election' *Journal of Eastern African Studies*, 2024.

Modreanu S, 'The post-truth era?' *Human and Social Studies*, 2017.

Maweu J, "'Fake elections"? Cyber propaganda, disinformation and the 2017 general elections in Kenya' *Journal of African Media Studies*, 2020.

Roy D and Dutta M, 'A systematic review and research perspective on recommender systems' *Journal of Big Data*, 2022.

Fernández M, Bellogín A, and Cantador I, 'Analysing the effect of recommendation algorithms on the amplification of misinformation' *arXiv*, 2021.

Montoro-Montarroso A et al., 'Fighting disinformation with artificial intelligence: fundamentals, advances and challenges' *Profesional de la Información*, 2023.

Lamo M and Calo R, 'Regulating bot speech' *UCLA Law Review*, 2018.

Sengar S, Hasan A, Kumar S, and Carroll F, 'Generative artificial intelligence: a systematic review and applications' *Multimedia Tools and Applications*, 2024.

Reports

The Kofi Annan Commission on Elections and Democracy in the Digital Age, *Protecting electoral integrity in the digital age*, 2020.

KICTANet, *Fake news, dangerous speech and the elections: Talk to NCIC – KICTANet community engagement report*, 2017.

European Commission, *Tackling Online Disinformation: A European Approach*, 2018.

Centre for Intellectual Property and Information Technology Law (CIPIT), *Biometric technology, elections, and privacy: Investigating privacy implications of biometric voter registration in Kenya's 2017 election process*, 2017.

Online Sources

Ndlela M, 'Algorithms, bots and elections in Africa: how social media influences political choices' *The Conversation*.

Feuer W, 'Cambridge Analytica and its role in Kenya's 2017 elections' *CNBC*, 23 March 2018.

Madung O, *From dance app to political mercenary: How disinformation on TikTok gaslights political tensions in Kenya*, Mozilla Foundation, 2022.

Stepney E and Lally C, 'Disinformation: sources, spread and impact' *POSTnote*.

Working Papers

Martin-Rozumilowicz B and Kuzel R, 'Social media, disinformation and electoral integrity' *IFES Working Paper*.