



Deepfakes, Electoral Integrity, and Constitutional Democracy: Rethinking Freedom of Expression in the Digital Era

M. Razia Begum

Assistant Professor in law, Sultan-ul-uloom College, Osmania University, Hyderabad, India.

Abstract

The rapid advancement of artificial intelligence has enabled the creation and dissemination of highly realistic deepfake content, creating significant challenges for electoral integrity and constitutional democracy. This paper critically examines the impact of deepfakes on democratic elections, with particular emphasis on the constitutional tension between safeguarding electoral processes and protecting freedom of expression. Adopting a qualitative, interpretivist and inductive approach, the research relies on secondary data comprising academic literature, legislation, judicial decisions, governmental reports and policy documents, analysed through thematic analysis. The paper finds that deepfakes can facilitate political misinformation, voter manipulation, identity impersonation and declining public trust, while existing legal frameworks remain insufficiently specific to address election-related synthetic media. A comparative assessment of India, the European Union, the United Kingdom and the United States demonstrates significant differences in legislative clarity, platform accountability and election-specific regulation. The research further establishes that excessive regulation may suppress legitimate political expression, whereas inadequate regulation may undermine informed democratic participation. It therefore advocates a proportionate constitutional approach based on clear and dedicated deepfake election legislation, stronger platform accountability and transparency, technological detection, digital literacy, judicial oversight and international regulatory cooperation. Such measures can strengthen electoral integrity while preserving the fundamental democratic value of freedom of expression in the digital era.

Keywords: Deepfake Technology; Electoral Integrity; Constitutional Democracy; Freedom of Expression; Political Misinformation.

1. Introduction

The rapid advancement of artificial intelligence (AI) has transformed the digital communication process, as it has become easier to make realistic images, audio and videos called deepfakes. These technologies have some good opportunities in terms of education, the development of entertainment and media and cost reduction of production (Aagaard & Marthedal, 2023). Despite these advantages that prove the ability of AI as something innovative, this technology may also be exploited to manipulate facts and disseminate fake political news. This has raised growing concerns about the effect of deepfakes in democratic elections and citizen confidence.

The integrity of the voting process requires that voters are accurately informed to make sound political decisions. However, the art of deepfakes has made it very difficult to differentiate and separate real and fake



International Journal of Law, Politics and Governance (IJLPG)

Volume 1 | Issue 1 | 2026 | Article ID: 8754-8849-1920 | <https://doi.org/10.64823/ijlpg.2601010>

IORO Publications · Texas, USA · www.ioro.org

content, especially when it comes to election times, and misleading information can be quickly shared by social media. This brings up crucial constitutional issues as to whether freedom of expression should take precedence over safeguarding democratic processes. Whereas over-regulation can limit the legal speech of political activists, weak regulation can cause harmful misinformation to be used to shape election results. Therefore, the paper considers the way constitutional democracies should react to the increasing threat of deepfakes and remain able to safeguard the basic right to digital-age freedom of expression.

Deepfakes have raised major legal and constitutional issues due to the struggle of current laws to react quickly to the constantly evolving methods of AI-generated political fake news. Although freedom of expression is one of the constitutional rights, the abuse of deepfakes can lead to a loss of electoral integrity through deceiving voters and decreasing public trust towards democratic institutions. However, the introduction of tougher regulation can also raise some issues regarding censorship and unwarranted limitations of legitimate political speech (Ali *et al.*, 2021). Therefore, constitutional freedoms lead to the challenging responsibility of governments to safeguard democratic elections without threatening constitutional freedoms. The lack of obvious juridical norms and consistent regulatory approaches emphasises the necessity to investigate whether present constitutional and legal frameworks can help to mitigate the dangers posed by deepfake technology.

The aim of this paper is to critically analyse how electoral integrity and constitutional democracy are affected by the deepfake technology, as well as the consideration of how the freedom of expression can be balanced with the beneficial legal and regulatory actions in the digital era.

1.1.1. Objectives

- To research how deepfake technology affects electoral integrity and democratic elections.
- To examine the relationship between freedom of expression and the regulation of AI-generated political misinformation in the constitution.
- To critically analyse legal and regulatory frameworks addressing deepfakes in constitutional democracies.
- To provide legal and policy recommendations that balance freedom of expression and protection of electoral integrity.

1.2. Research Questions

- **RQ1** - What is the impact of deepfake technology on electoral integrity within constitutional democracies?
- **RQ2** - What constitutional challenges arise when regulating deepfake-generated political content while protecting freedom of expression?
- **RQ3** - How effective are existing legal and regulatory frameworks in addressing the risks posed by deepfake technology during elections?
- **RQ4** - What legal and policy measures can better balance freedom of expression with the protection of electoral integrity in the digital era?

The use of deepfake technology in political campaigns has become a significant issue of defensive priority in terms of defending the election process in a democratic environment, as well as constitutional rights. Even though some research has been conducted on deepfakes so far, technologically and media-wise, the studies that have been carried out have not critically investigated how constitutional democracies can restrict AI-created political misinformation and the weakening of freedom of expression. This offers a significant research gap as legal systems have to deal with the new types of digital risks and still should ensure core

rights. Therefore, this paper has importance as it critically reviews the connection between deepfakes, electoral integrity and constitutional democracy, and outlines legal and policy strategies that aim to reconcile the protection of democracy with freedom of expression in the digital age.

This paper focuses on the constitutional and legal issues that deepfake technology has created concerning electoral integrity and freedom of expression. It studies scholarly articles, laws, case law, governmental reports and policy documents to assess the current legal and regulatory responses in constitutional democracies. The research is mainly focused on secondary qualitative data and does not involve primary data collection through interviews or surveys. Although deepfakes are used in many sectors, this paper specifically focused on political communication, democratic elections, as well as constitutional rights.

2. Literature Review

2.1 Introduction

Deepfake technology has emerged as a significant field of law and academic discussion due to its increasing impact on political communication and democracy. The available literature discusses the opportunities that artificial intelligence has opened as well as the dangers of digitally manipulated content, especially when it comes to elections (Basol *et al.*, 2021). However, there is no clear agreement on how constitutional democracies should control deepfakes without limiting the freedom of expression. This paper critically examines the current literature and determines the key debates on which the current research will be based.

2.1. 2.2 Understanding Deepfake Technology and Digital Misinformation

Deepfake technology is widely recognised as one of the most significant developments in artificial intelligence since it can produce high-quality realistic images, videos and audio that can seriously resemble real people. According to Bassini (2025), the innovation has reengineered digital communication by endorsing education, entertainment, news and creative powers. The technology is able to enhance accessibility, lower production costs and promote innovation in various industries (Cavaliere, 2024). In this sense, deepfakes cannot be considered only a harmful tool since the usefulness of such technology is mostly based on the motive of creation and usage.

However, Brashier *et al.* (2021) argue that this optimistic interpretation has been criticised because it fails to consider the reality of the practical effects of wide-scale digital manipulation. Thus, when claiming that deepfake technology is neutral, it neglects the increased social dangers of distributing fake information.

Chawki (2025) makes a critical argument that a more balanced approach shows that the greatest concern is not the technology itself but the broader digital environment, within which it functions. In this situation, any false material can be distributed to a significant number of people without fact-checking and deterring the dissemination of fake news becomes even more complicated (Chawki, 2025). Innovation can be reduced without limiting its advancement by employing technological interventions like AI detection systems, digital watermarking and content authentication.

Overall, deepfake technology has its opportunities and some serious challenges; the literature confirms this idea. Chen *et al.* (2025) summarise that as much as innovation is contributing to economic and technological developments, it needs to be used appropriately, and its abuse has created emerging concerns about digital misinformation and trust. The existing literature and discussions are usually centred on technological solutions, but they give little consideration to the constitutional and legal impacts of governing political

content that is created by AI (Chung & Kim, 2021). This shows that there is still a necessity to explore further how legal frameworks can act adequately and, at the same time, maintain the principles of democracy and the freedom of expression.

2.2. 2.3 Deepfakes and Electoral Integrity

Electoral integrity is defined through free, fair and informed democratic participation, and thus access to correct political information during the election campaigns is crucial. In this sense, deepfakes pose a very critical threat to democratic legitimacy by lowering overall trust in the electoral procedures and creating ambiguity related to the validity of political discourses.

However, Cotter et al. (2021) argue that the impact of deepfakes on election outcomes can be overstated. They propose that political misinformation is not a new development created by artificial intelligence and that voters tend to discuss the information based on their own political preconceptions and not accept the online information without challenge (Dame Adjinn-Tettey, 2022). Thus, deepfakes must be viewed as a part of a broader misinformation system, not as the primary reason behind the decreasing level of electoral confidence.

A more balanced perspective acknowledges that the influence of deepfakes depends on political, legal and technological factors. The presence of strong electorally-based institutions, independent media, and fact-checking systems in countries can be in a better position to diminish the power of manipulated information (De Gregorio & Pollicino, 2025). This indicates that institutional resilience in itself might not offer adequate security against more realistic AI-generated political content.

Overall, the literature agrees that maintaining electoral integrity requires more than simply removing false digital content. Douek (2021) states that technological detection and platform moderation can help reduce direct risks, but do not adequately confront broader constitutional issues related to democratic participation and political freedom. Current literature is still debating the extent of the threat but has limited focus on how laws are recommended to maintain the balance between the protection of elections and the fundamental right (Ecker et al., 2022).

2.3. 2.4 Freedom of Expression in Constitutional Democracies

The freedom of expression is generally accepted as one of the basic principles of constitutional democracy since individuals can voice their opinion, engage in political discourse and hold governments accountable. Ecker et al. (2020) have asserted that safeguarding political speech is vital in free and fair elections as voters need to be exposed to a variety of opinions in order to make informed choices. Freedom of expression is therefore considered a pillar of constitutional governance.

However, Ferrara (2024) argues that this method has been criticised for paying inadequate focus to the damage caused through intentionally false or manipulated political material. Thus, according to the critics of this idea, the very freedom of expression cannot be safeguarded without taking into account misuse, as it can be weakened instead, and democratic values can be reinforced.

A more moderate view held by Gillespie (2022) maintains that constitutional democracies should neither allow the free flow of deepfakes nor implement excessive censorship. However, it is a large-scale legal issue to establish the point at which political speeches become unlawful and when some speech starts to pose a harmful threat.

Overall, the literature allows concluding that the freedom of expression and the protection of elections are one of the most intricate constitutional challenges that deepfake technology poses. In contrast, weak

regulation can enable harmful content to discourage people from participating in the voting process (Gonçalves et al., 2023). Current studies on the subject matter thus offer no general answer to this constitutional dilemma, signifying the necessity to consider how legal frameworks can safeguard not only fundamental privileges but democratic stability in the digital era.

2.4. 2.5 Existing Legal and Regulatory Frameworks

Jurisdiction	Major Law	Primary Focus	Limitation
India	IT Act 2000	Cyber offences	No deepfake provisions
India	DPDP Act 2023	Data privacy	Election issues not covered
India	Representation of the People Act 1951	Electoral conduct	No AI regulation
EU	AI Act	AI transparency	Limited election provisions
EU	Digital Services Act	Platform accountability	Enforcement challenges
UK	Online Safety Act 2023	Harmful online content	AI-specific rules limited
USA	First Amendment	Free speech	Fragmented state regulation

Table 1: Summary of Legal Frameworks

Most constitutional democracies have proposed legal regulations which can indirectly control the exploitation of deepfake technology, especially in the election process. In India, under the provisions of the Information Technology Act 2000, Digital Personal Data Protection Act 2023 and applicable provisions of the Bharatiya Nyaya Sanhita 2023 provisions may be utilised whereby, in case of deepfakes, there is misuse of identities, misinformation or harm of individuals. Similarly, the European Artificial Intelligence Act takes the form of a risk-based stance by ensuring that AI-generated content and data are open to view, whereas the Digital Services Act empowers online platforms to be more responsible towards addressing illegal and harmful online content.

However, Guay et al. (2023) argue that such legal systems are not comprehensive since most have not been specifically structured to control deepfake. In India, before the emergence of other sophisticated forms of generative AI, the Information Technology Act 2000 was enacted, and it is not clear how it applies to more sophisticated forms of political deepfakes (Guerrero-Sierra et al., 2025). Similarly, even though the Digital Personal Data Protection Act 2023 is an improvement in protecting privacy, it does not directly control AI-generated political misinformation in campaign activities. The same issues can be raised on the global level, where the main responsiveness of the EU Artificial Intelligence Act is transparency issues, but not election-specific regulation.

A more moderate viewpoint provided by Haenschen (2023) is that legal regulation alone will not be sufficient to counterbalance the issues posed by deepfakes. One example is that the United States has mainly trusted to state-level legislation, including legislation in California concerning deceptive election deepfakes, and advocated voluntary behaviour by digital platforms instead of introducing comprehensive federal legislation (Haimson et al., 2021). Even though such solutions are more flexible, lacking legal uniformity within different

jurisdictions could decrease their usefulness, especially since misinformation online can readily break national borders.

Overall, the literature shows that some serious steps towards regulation of AI-generated misinformation have been taken, but there are still large gaps in the law. Despite the current laws offering valuable tools to deal with privacy breaches, impersonation, and digital content that cause an enduring harm, they do not actually tackle the constitutional issues involved in dealing with election-related deepfakes.

2.5. 2.6 Theoretical Framework

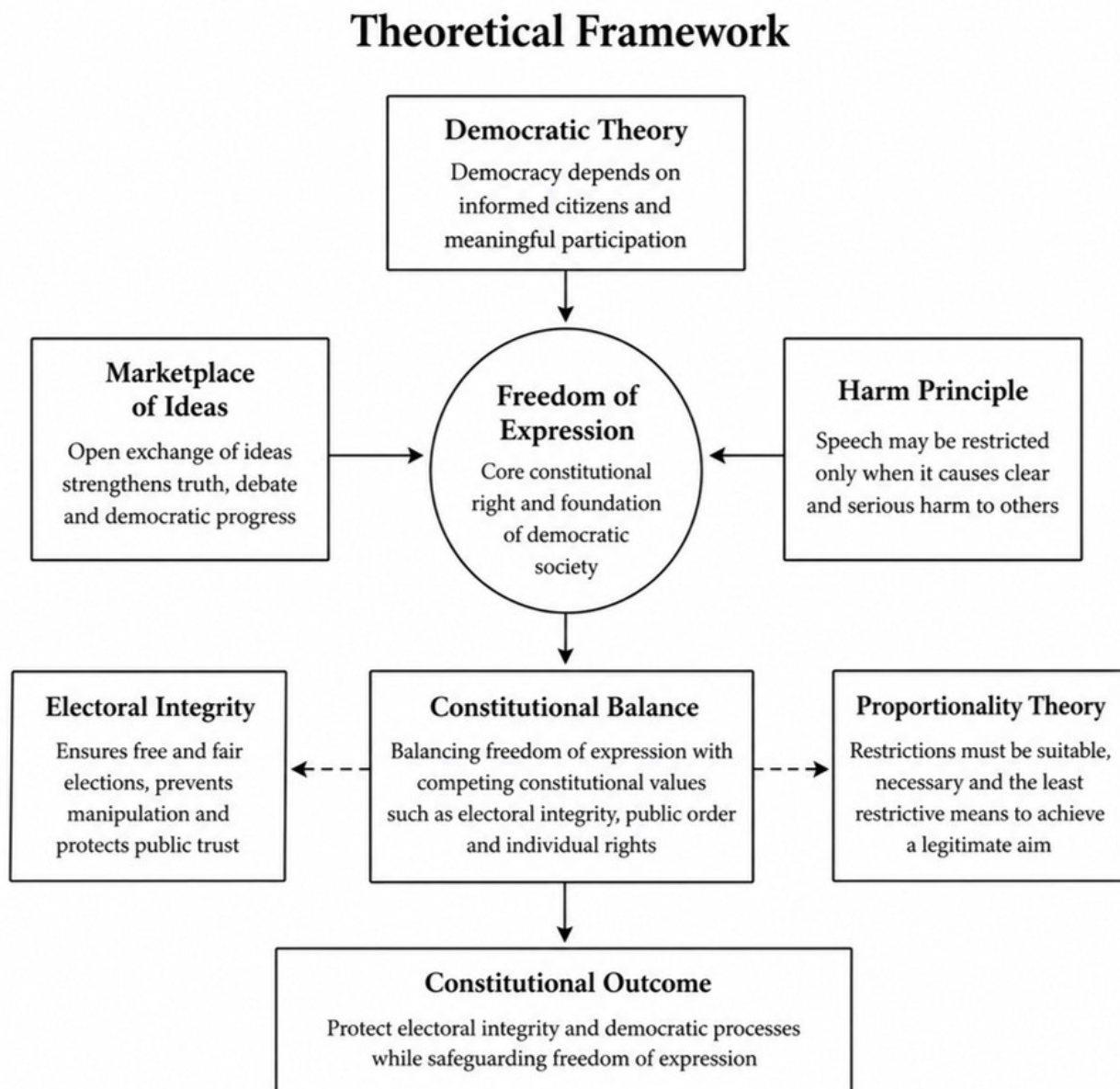


Figure 1: Theoretical Framework

This paper adopts multiple theoretical approaches to analyse the connection between deepfakes, electoral integrity and constitutional democracy. The Marketplace of Ideas Theory argues that free and open debate allows truth to emerge through the exchange of different opinions. In this light, the freedom of political expression should not be limited since democratic societies rely on free exchange of ideas (Heseltine &

Clemm von Hohenberg, 2024). The Democratic Theory also explains that informed public participation, transparent elections and political accountability are some of the requirements of democratic legitimacy. Mill's Harm Principle Theory that suggests that personal freedom can only be restricted to limit a situation that might harm others, is also applied in the paper. Even though this principle grants freedom of speech, it is also used to grant constitutional ground for the regulation of harmful deepfake content in an election or a country where this content poses a threat to the integrity of elections or a democratic system.

2.6.

2.7. 2.7 Conceptual Framework

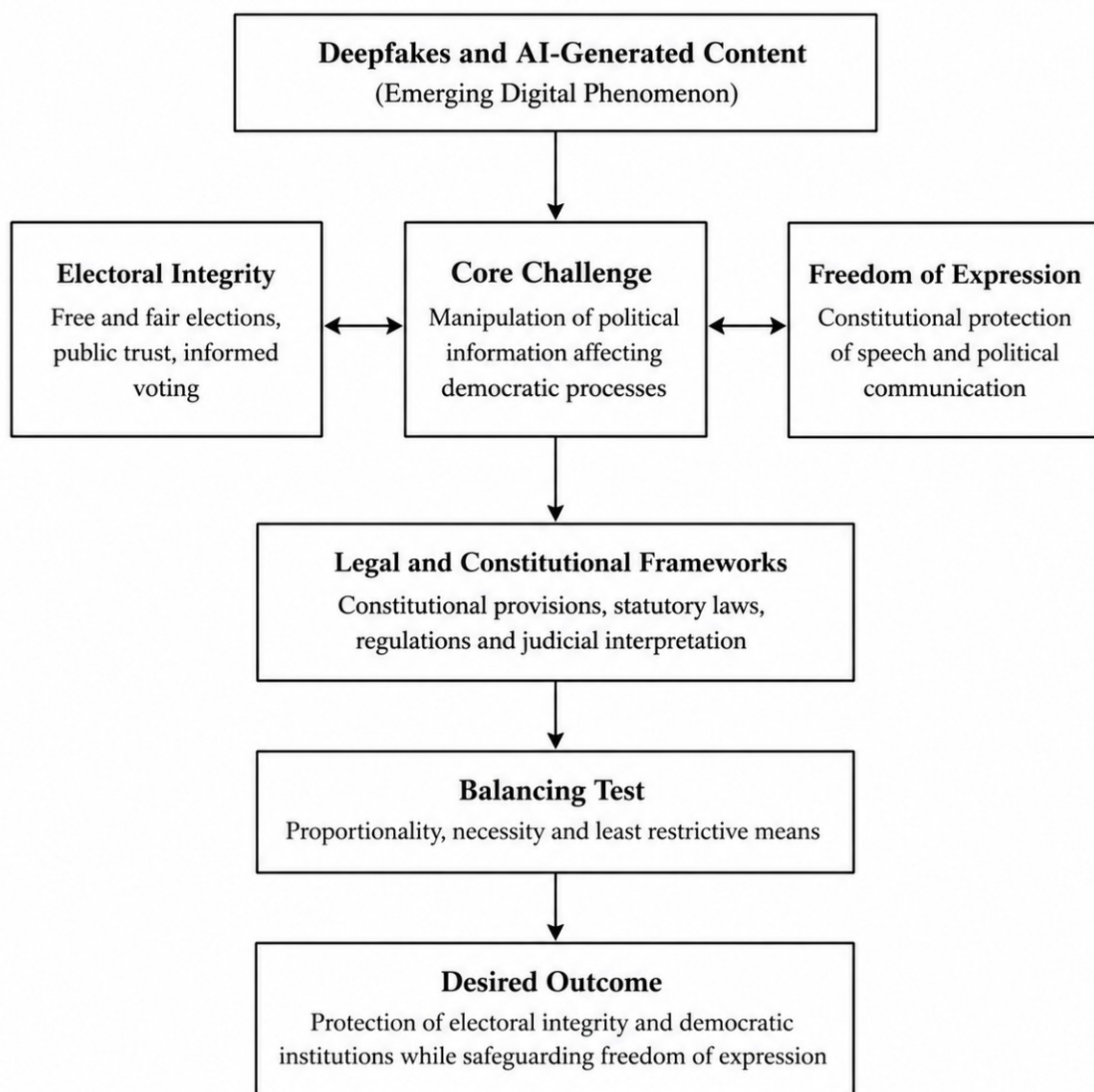


Figure 2: Conceptual Framework

The conceptual framework describes the connection between the key ideas that are being discussed in this paper. The interaction of these concepts affects the broader operation of constitutional democracy where governments have to balance individual freedoms with the safeguarding of fair elections.

2.8. 2.8 Literature Gaps

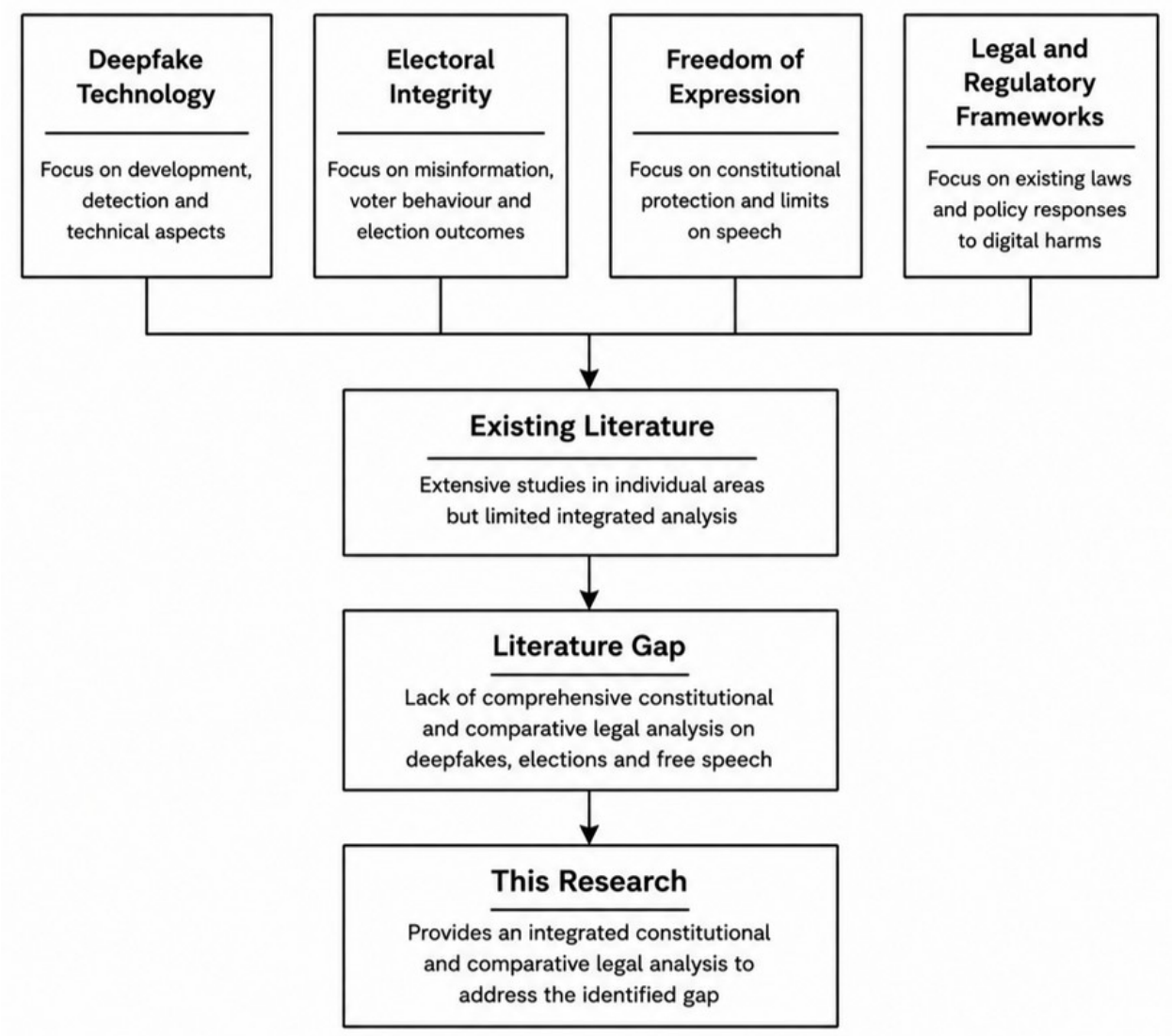


Figure 3: Literature Gaps

The reviewed literature provides valuable insights into deepfake technology, digital misinformation and freedom of expression. Hence, future studies should aim to critically analyse a wider range of constitutional democracies to present a balanced response to legal issues that allocates sufficient protection to electoral integrity and fundamental rights in the digital age.

3. Methodology

This chapter outlines the research methodology used to analyse the association between deepfakes, electoral integrity and constitutional democracy (Kruikemeier et al., 2026). The philosophy of research, approach, design, data collection, data analysis, reliability, ethical considerations and research limitations are also discussed to ensure that the study is conducted in a systematic and academically rigorous manner.

3.1. 3.1 Research Type

This study adopts a qualitative research methodology as it allows a thorough investigation of the legal principles, constitutional arguments and scholarly points of view concerning the issue of deepfakes, electoral integrity and the freedom of speech. A qualitative study is most appropriate in problem-based research where numerical measurement significantly lacks importance as compared to interpretation and critical analysis of law (Lavigne, 2021). It also enables the paper to compare the legislation, the case law and the academic literature of various constitutional democracies. However, quantitative research is mostly used in connection with statistical analysis and numerical data, which is less suitable in the case of studying the interpretation of the constitution and law reasoning. Therefore, qualitative research would be the most suitable method to fulfil the purpose of the study.

3.2. 3.2 Research Philosophy

This study adopts an interpretivist research philosophy since it favours interpretation of law provisions, legal rights and the scholarly discussions that revolve around the area of deepfakes and the freedom of expression. Interpretivism acknowledges legal issues constructed through social, political and constitutional situations, and this means the research can evaluate critically various perspectives and not discover an objective truth (Lee & Ramazan, 2021). Therefore, this qualitative secondary type of research is best supported by interpretivism as the best philosophy.

3.3. 3.3 Research Approach

The research approach applied in this study is an inductive research approach, as it enables the formulation of conclusions on the basis of the analysis of the existing legal literature, case law, and policy documents in the area of deepfakes and constitutional democracy (Lee et al., 2023). Therefore, this qualitative secondary study needs the most fitting approach, which is the inductive one.

3.4. 3.4 Research Design

This study employs an exploratory research design since it deals with a new legal issue and current knowledge on the issue is still evolving. A design that aids this goal is exploratory, which will promote a thorough study of legislation, case law and scholarly publications. Therefore, an exploratory design would be the best option when it comes to answering the goals of this study.

3.5. 3.5 Research Strategy

The present study incorporates a secondary research approach which is founded on systematic analysis of academic sources, law, case law, governmental reports and government policy documents. This design suits well as it can allow the study to critically assess the current body of knowledge and compare legal responses in various constitutional democracies without having to collect primary data (Lewandowsky & Pomerantsev, 2022). Therefore, a secondary research strategy is the most suitable.

3.6. 3.6 Data Collection Methods

This study uses secondary data collection methods as it is appropriate due to the possibility of reviewing the already existing legal and academic data that applies to deepfake technology, electoral integrity, and constitutional democracy. Peer-reviewed journal articles, books, legislation, case law, government reports, and policy documentation of established international organisations are used to gather the data (Lewandowsky & Van Der Linden, 2021). Thus, the secondary data collection is regarded as the most

appropriate one since it will help to conduct a thorough legal analysis relying on trustworthy and thoroughly proven sources.

3.7. 3.7 Research Limitations

The study relies exclusively on secondary sources and therefore does not capture the latest views of practitioners, policymakers or voters. Nevertheless, scholarly, legislative, judicial and governmental sources provide a sound basis for analysing the legal and constitutional concerns surrounding deepfakes and elections.

4. Thematic Analysis of Secondary Data

4.1. Theme One: Deepfakes as a Threat to Electoral Integrity

The thematic analysis reveals that deepfake technology is a major threat to the integrity of elections because it reveals the vulnerability in the legal procedures addressing political communication (Minici et al., 2024). In India, the Representation of the People Act 1951 governs electoral behaviour and is intended to promote fair and unbiased elections, yet it does not have any particular statements regarding AI-generated political misinformation or synthetic media. In the same way, the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023 protect against cybercrimes, identity fraud and personal information crimes, but do not explicitly prohibit producing or spreading election-related deepfakes.

The European Union AI Act proposes disclosure of specific information about AI-generated material, whereas the Digital Services Act reinforces the role of the Internet platform in eliminating unlawful or harmful content. Similarly, the United Kingdom Online Safety Act 2023 also imposes a heavier responsibility on online platforms to minimise damaging online content. Despite the positive steps of these legal evolutions, special attention is paid to accountability and transparency of platforms, but it does not create strict regulations of election-related deepfakes.

Another finding is that lawful protection of political speech in the constitution leads to greater legal complexity (Nguyen et al., 2025). Article 19(1)(a) of the Indian Constitution provides an entitlement to freedom of speech and expression, but Article 19(2) allows that restrictions can be made when the interest of the public order, defamation and other established reasons exist. In the same way, Article 10 of the European Convention on Human Rights and the First Amendment of the United States Constitution highly secure freedom of expression. Even though these constitutional protections are fundamental to the rule of law, they do not help in controlling deceptive political messages easily, which in turn raises issues regarding censorship or the overreaching role of the government.

4.2.

4.3. Theme Two: Constitutional Protection of Freedom of Expression in the Digital Era

The thematic analysis shows that freedom of expression has been among the safest constitutional rights in democratic societies, but with the advent of deepfake technology, it has questioned the legal boundaries of such a right (Nguyen et al., 2022). Article 19(1)(a) of the Constitution of India provides every citizen with the right to freely communicate and speak, as they acknowledge open political dialogue is vital to democratic government. The case *Shreya Singhal v Union of India* (2015) reinforced this idea, stressing that any measure

to limit online speech should be reasonable and justified under the Constitution. Likewise, Article 10 of the European Convention on Human Rights (ECHR) and the First Amendment of the United States Constitution heavily safeguard political expression as evidence of the significance of free, open discussions in the election period.

However, the analysis points out that free speech as safeguarded by the Constitution does not grant a free hand to spread misconstrued or misleading political materials (Nyhan et al., 2020). Article 19(2) of Indian constitution allows that freedom of expression can be limited reasonably in the interests of protecting the integrity and Sovereignty of the state, defamation, decency and morality. Similarly, Article 10 (2) of the ECHR permits restrictions where such is essential in a democratic society so as to safeguard the rights of others or to preserve order in the society. These constitutional clauses imply that despite the high level of legal protection given to political speech, governments have been enabled to control harmful speech where a considerable constitutional purpose exists.

The analysis also indicates that judicial interpretation is important in balancing the constitutional rights against the interests of the people. *Puttaswamy (Retd.) v Union of India* (2017), the Supreme Court recognised privacy as a fundamental right per Article 21 in the strengthening of the constitutional right to the dignity of the individual and the autonomy of the personality. This shows that constitutional rights cannot be defined separately, but they have to be viewed in relation to the other basic rights and democratic principles.

4.4. Theme Three: Balancing Electoral Integrity with Freedom of Expression

The freedom of expression or electoral integrity may be at risk in such a way that it becomes one of the most serious constitutional problems due to deepfake technology (Pennycook & Rand, 2021). Even in India, under the Constitution, freedom of speech is secured by Article 19(1)(a), and it is allowed to be restricted in reasonable ways in Article 19(2) where it is inevitable to safeguard the legitimate interests of people. Therefore, even the Constitution admits that the rights of individuals and the interests of the state cannot conflict but need to coexist.

However, the analysis shows that anything that could guarantee this constitutional balancing is much more complicated in reality. Extensive legal bans on deepfakes can ensure that, accidentally, deepfakes, legitimate political criticism, investigative journalism, and open discussion, which are critical elements of constitutional democracy, are discouraged (Porter & Wood, 2021). In *Shreya Singhal v Union of India* (2015), the Supreme Court of India reiterated that unclear or excessively broad areas of limitation on online expression might contravene constitutional guarantees in Article 19(1)(a). In a similar manner, the First Amendment to the United States Constitution has an exceptional protection of political speech, one of the judicial precautions taken against overreaching violations in governance. Such approaches to the Constitution suggest that whereas deepfakes pose real dangers, governments should not establish statutes that create uncertainty or suppress expression within democracy.

The thematic analysis also indicates that an increase in the number of jurisdictions favours a proportionate approach to regulation over absolute prohibition (Radesky et al., 2024). The European Union AI Act facilitates transparency by ensuring that some AI-generated materials are clearly identified, and the Digital Services Act empowers responsible AI platforms by enhancing their control of how illegal or false online content is handled. Similarly, the United Kingdom Online Safety Act 2023 urges online platforms to limit harmful material without resorting to bans on legal expression. However, the variations in the national constitutional

systems still bring irregularity in the legal requirements, especially when considering that the scope of protection of political speech should be differently enforced.

4.5. Theme Four: Emerging Legal and Regulatory Responses to Deepfakes

The thematic analysis shows that constitutional democracies are introducing more legal and regulatory tools to deal with the risks of deepfake technology. The legal mechanisms in India are the Information Technology Act 2000, the Digital Personal Data Protection Act 2023 and the Bharatiya Nyaya Sanhita 2023, which could be utilised in cases of deepfakes in which identity misuse, violation of privacy or other cyber-related crimes were used. Across the globe, the European Union AI Act, the Digital Services Act and the United Kingdom Online Safety Act 2023 all evidence an increased desire to enhance transparency and intensify the accountability of digital platforms.

However, the discussion above reveals that these frameworks are still incomplete since most of them were established prior to the global explosion of generative artificial intelligence, and thus fail to regulate election-related deepfakes in full. Therefore, a combination of unclear statutory language and the doubt concerning the broader applicability of the law enabled enforcement solely based on the interpretation of the existing laws (Rana et al., 2022). This finding recommends that in future legislative changes, reasonable and coordinated legal regulations should be considered that are capable of ensuring electoral integrity without violating constitutional protections of freedom of expression.

The thematic analysis identified four connected issues: deepfakes threaten electoral integrity; freedom of expression remains constitutionally protected; regulation must balance democratic protection with speech rights; and existing legal frameworks remain incomplete. These findings provide the basis for the discussion of proportionate legal reform.

This paper examined the secondary evidence based on four themes, which are all connected to that of deepfakes, electoral integrity, freedom of expression and legal regulation. These findings provide the foundation for the next paper, which discusses the results in relation to the research questions, theoretical framework and wider constitutional principles.

5 Discussion

This section of the paper contains the interpretation of the findings in terms of the objectives of the research, theoretical framework and the broader constitutional principles. The study on the influence of deepfake technology on electoral integrity, freedom of expression and constitutional democracy in various jurisdictions is critically assessed (Roozenbeek et al., 2021). The results show that deepfake technology has changed the legal environment of democratic elections to a great extent, as it causes the threat of distorted political communication to rise. Even though electoral law, like the Representation of the People Act 1951 in India, is meant to ensure free and fair elections, it was formulated earlier than the advent of advanced artificial intelligence and thus offers limited focus on AI-generated political misinformation. This shows that electoral regulation is not enough anymore to deal with new emerging threats to democratic processes.

These results are also in line with the Democratic Theory, which maintains that the legitimacy related to democracy rests on active participation in politics and the trust of people in the electoral institution. However, the evidence suggests that technological innovation cannot be taken only as a threat, as artificial

intelligence could develop opportunities to enhance communication and interaction with the population in the case of responsible use. Therefore, the main constitutional problem is not to stop technological advancement but to make sure that the legal framework can address the changes so that it can guarantee the integrity of elections and facilitate a democratic process.

The findings suggest that the regulation of deepfake technologies can be rather problematic on the constitutional level, as governments should keep up with the fast-paced effects of digital activities and consider essential rights. Article 19(1)(a) of the Constitution of India guarantees the right to speech and expression, and in the same section, Article 19(2) allows reasonable limitations when it is required to promote legitimate public interests. The same issues can be observed in the European Union, where the AI Act and the Digital Services Act advance transparency and accountability of platforms, but still fail to fully address all types of AI-driven political manipulation.

These results help substantiate Mill's Harm Principle that states that individual liberty can only be limited in cases where it cannot cause harm to others. A proportionate legal approach remains essential for preserving both constitutional rights and electoral integrity.

The findings imply that it is time to shift the legal treatment of AI-related political misinformation off the back of the current cyber and electoral laws and the creation of specific instruments to address AI-related political misinformation. Particular laws that regulate election-related deepfakes are not established in India; however, there are partial legal measures in the form of the Information Technology Act 2000, the Digital Personal Data Protection Act 2023, the Bharatiya Nyaya Sanhita 2023, the Representation of the People Act 1951. The deepening of a legal context would give courts, electoral bodies and online platforms even more legal clarity and would increase the trust of citizens in democratic elections.

It was further shown that the policy in the future must incorporate a co-operative approach among governments, electoral commissions, technology companies and civil society organisations (Simchon et al., 2024). Comparative analysis reveals that those measures that have been brought to the fore by the European Union AI Act, Digital Services Act and the United Kingdom Online Safety Act 2023 are more and more concerned with transparency, accountability of platforms and risk management. Therefore, AI detection should be encouraged by the legal change, digital literacy initiatives and even closer collaboration between the national and international regulatory bodies so that the constitutional rights could be secured along with the electoral integrity.

The results indicate that the concept of deepfake technology has wider consequences for constitutional democracy beyond data control, including information and misinformation that goes online. This paper will therefore recommend that constitutional democracies should embrace legal action that safeguards the integrity of the elections and basic rights. Finally, to enhance constitutional democracy protection in the long term, the introduction of new laws, as well as maintaining a flexible, transparent and responsive legal framework to future developments in technology, is crucial.

The discussion demonstrates that existing legal approaches provide important safeguards but remain inadequate for election-related deepfakes. Constitutional theory and comparative analysis support proportionate reform that protects electoral integrity without unnecessarily restricting fundamental rights.

This paper interpreted the findings by looking at how the findings were interpreted in terms of constitutional and legal implications as far as electoral integrity, freedom of expression and democratic governance were concerned. The discussions form the foundation of the conclusions and recommendations given in the last paper.

6 Conclusion and Recommendations

The paper took a critical look at the effects that deepfake technology has on electoral integrity and constitutional democracy, and how freedom of expression can be harmonised with sufficient legal and regulatory responses. Laws in force in India such as the Representation of the People Act 1951, the Information Technology Act 2000, the Digital Personal Data Protection Act 2023 and the Bharatiya Nyaya Sanhita 2023 have partial coverage but fail to thoroughly regulate election-based deepfakes. The research questions were addressed by proving that the only way to help through effective regulation is to have a balanced constitutionalism that helps to secure democratic elections and freedom of expression with legal measures that are clear and proportionate to what technology demands.

4.5.1. Recommendation One - Introduce Dedicated Deepfake Election Legislation

During election time, governments need to implement a bill specifically dealing with the development and sale of AI-generated political content. In India, legal clarity on deepfakes related to election may be defined by amending the Representation of the People Act 1951 and the Information technology Act 2000 which could specify unauthorised acts to prevent unwarranted interference with elections and to enter proportionate punishments on deliberate interruptions with elections (Umbach et al., 2024). Specific laws would help eliminate legal ambiguity, as they would eliminate the need to use the general clauses of statutory law and would include regulations specifically on AI technologies.

4.5.2.

4.5.3. Recommendation Two - Strengthen Platform Accountability and Transparency

Digital platforms should be subject to stronger legal obligations to identify, label and respond promptly to AI-generated political content (Walter et al., 2020). Regulatory strategies that have been embraced as part of the European Union AI Act and the Digital Services Act reflect the importance of transparency and platform responsibility to limit the proliferation of detrimental misinformation. The same approach might be used to a greater extent by demanding that technology companies return to using more reliable detection mechanisms, have open content moderation processes and collaborate with electoral bodies during elections.

4.5.4.

4.5.5. Recommendation Three - Promote International Regulatory Cooperation

Digital communication is cross-border, and it needs increased collaboration between governments, electoral bodies and international bodies. Increased cross-border cooperation would enhance the integrity of elections and constitutional safeguards of freedom of expression.

The new regulations of AI should be investigated in terms of their long-term effectiveness in the future, as constitutional democracies are still re-adapting to the technological changes. Moreover, an empirical investigation among legal professionals, policymakers, electoral organisations and technology firms may offer empirical data that may support the secondary evidence offered in this paper.

References

- [1] Aagaard, P., & Marthedal, S. (2023). Political microtargeting: Towards a pragmatic approach. *Internet Policy Review*, 12(1), 1-22. <https://www.econstor.eu/handle/10419/271329>.
- [2] Ali, M., Sapiezynski, P., Korolova, A., Mislove, A., & Rieke, A. (2021, March). Ad delivery algorithms: The hidden arbiters of political messaging. In *Proceedings of the 14th ACM international conference on web search and data mining* (pp. 13-21). <https://dl.acm.org/doi/abs/10.1145/3437963.3441801>
- [3] Basol, M., Roozenbeek, J., Berriche, M., Uenal, F., McClanahan, W. P., & Linden, S. V. D. (2021). Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation. *Big Data & Society*, 8(1), 20539517211013868. <https://journals.sagepub.com/doi/abs/10.1177/20539517211013868>
- [4] Bassini, M. (2025). Speech without a speaker: Constitutional coverage for generative AI output?. *European Constitutional Law Review*, 21(3), 375-411. <https://www.cambridge.org/core/journals/european-constitutional-law-review/article/speech-without-a-speaker-constitutional-coverage-for-generative-ai-output/68F18876ED0C4C34B0D301ADE52CD821>
- [5] Brashier, N. M., Pennycook, G., Berinsky, A. J., & Rand, D. G. (2021). Timing matters when correcting fake news. *Proceedings of the National Academy of Sciences*, 118(5), e2020043118. <https://www.pnas.org/doi/abs/10.1073/pnas.2020043118>
- [6] Cavaliere, P. (2024). Freedom of expression after disinformation: Towards a new paradigm for the right to receive information. *Journal of Media Law*, 16(1), 28-37. <https://www.tandfonline.com/doi/abs/10.1080/17577632.2024.2362482>
- [7] Chawki, M. (2025). AI moderation and legal frameworks in child-centric social media: a case study of Roblox. *Laws*, 14(3), 29. <https://www.mdpi.com/2075-471X/14/3/29>
- [8] Chen, Z., Ye, J., Tsai, B., Ferrara, E., & Luceri, L. (2025, September). Synthetic politics: Prevalence, spreaders, and emotional reception of AI-generated political images on X. In *Proceedings of the 36th ACM Conference on Hypertext and Social Media* (pp. 11-21). <https://dl.acm.org/doi/abs/10.1145/3720553.3746675>
- [9] Chung, M., & Kim, N. (2021). When I learn the news is false: How fact-checking information stems the spread of fake news via third-person perception. *Human Communication Research*, 47(1), 1-24. <https://academic.oup.com/hcr/article-abstract/47/1/1/5917727>
- [10] Cotter, K., Medeiros, M., Pak, C., & Thorson, K. (2021). "Reach the right people": The politics of "interests" in Facebook's classification system for ad targeting. *Big Data & Society*, 8(1), 2053951721996046. <https://journals.sagepub.com/doi/abs/10.1177/2053951721996046>
- [11] Dame Adjin-Tetty, T. (2022). Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education. *Cogent arts & humanities*, 9(1), 2037229. <https://www.tandfonline.com/doi/abs/10.1080/23311983.2022.2037229>
- [12] De Gregorio, G., & Pollicino, O. (2025). The European constitutional way to address disinformation in the age of artificial intelligence. *German Law Journal*, 26(3), 449-470. <https://www.cambridge.org/core/journals/german-law-journal/article/european-constitutional-way-to-address-disinformation-in-the-age-of-artificial-intelligence/548C4C0592757ADC0D250EF8C4C3D434>
- [13] Douek, E. (2021). The limits of international law in content moderation. *UC Irvine J. Int'l Transnat'l & Comp. L.*, 6, 37. https://access.heinonline.com/hol/cgi-bin/get_pdf.cgi?handle=hein.journals/ucivitolm6§ion=6
- [14] Ecker, U. K., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., ... & Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature reviews psychology*, 1(1), 13-29. <https://www.nature.com/articles/s44159-021-00006-y>
- [15] Ecker, U. K., O'Reilly, Z., Reid, J. S., & Chang, E. P. (2020). The effectiveness of short-format refutational fact-checks. *British journal of psychology*, 111(1), 36-54. <https://bpspsychub.onlinelibrary.wiley.com/doi/abs/10.1111/bjop.12383>
- [16] Ferrara, E. (2024). Charting the landscape of nefarious uses of generative artificial intelligence for online election interference. *arXiv preprint arXiv:2406.01862*. <https://arxiv.org/abs/2406.01862>

- [17] Gillespie, T. (2022). Do not recommend? Reduction as a form of content moderation. *Social Media+ Society*, 8(3), 20563051221117552. <https://journals.sagepub.com/doi/abs/10.1177/20563051221117552>
- [18] Gonçalves, J., Weber, I., Masullo, G. M., Torres da Silva, M., & Hofhuis, J. (2023). Common sense or censorship: How algorithmic moderators and message type influence perceptions of online content deletion. *new media & society*, 25(10), 2595-2617. <https://journals.sagepub.com/doi/abs/10.1177/14614448211032310>
- [19] Guay, B., Berinsky, A. J., Pennycook, G., & Rand, D. (2023). How to think about whether misinformation interventions work. *Nature Human Behaviour*, 7(8), 1231-1233. <https://www.nature.com/articles/s41562-023-01667-w>
- [20] Guerrero-Sierra, H. F., Palacio Puerta, M., & Garavito Rincón, D. F. (2025). Threats and regulatory challenges of non-consensual pornographic deepfakes: an analysis of the colombian case. *Cogent Social Sciences*, 11(1), 2552342. <https://www.tandfonline.com/doi/abs/10.1080/23311886.2025.2552342>
- [21] Haenschen, K. (2023). The conditional effects of microtargeted facebook advertisements on voter turnout. *Political Behavior*, 45(4), 1661-1681. <https://link.springer.com/article/10.1007/s11109-022-09781-7>
- [22] Haimson, O. L., Delmonaco, D., Nie, P., & Wegner, A. (2021). Disproportionate removals and differing content moderation experiences for conservative, transgender, and black social media users: Marginalization and moderation gray areas. *Proceedings of the ACM on Human-computer Interaction*, 5(CSCW2), 1-35. <https://dl.acm.org/doi/abs/10.1145/3479610>
- [23] Heseltine, M., & Clemm von Hohenberg, B. (2024). Large language models as a substitute for human experts in annotating political text. *Research & Politics*, 11(1), 20531680241236239. <https://journals.sagepub.com/doi/abs/10.1177/20531680241236239>
- [24] Kruikemeier, S., Schäfer, S., Hamilton, A., Guldemon, P., Vrieling, J., Dymanus, C., ... & Boerman, S. C. (2026). AI meets politics: Examining the effects of different targeting strategies across 15 countries. *New Media & Society*, 28(7), 2932-2960. <https://journals.sagepub.com/doi/abs/10.1177/14614448261445063>
- [25] Lavigne, M. (2021). Strengthening ties: The influence of microtargeting on partisan attitudes and the vote. *Party Politics*, 27(5), 965-976. <https://journals.sagepub.com/doi/abs/10.1177/1354068820918387>
- [26] Lee, D. K. L., & Ramazan, O. (2021). Fact-checking of health information: The effect of media literacy, metacognition and health information exposure. *Journal of Health Communication*, 26(7), 491-500. <https://www.tandfonline.com/doi/abs/10.1080/10810730.2021.1955312>
- [27] Lee, S., Xiong, A., Seo, H., & Lee, D. (2023). "Fact-checking" fact checkers: A data-driven approach. *Harvard Kennedy School Misinformation Review*. <https://misinforeview.hks.harvard.edu/article/fact-checking-fact-checkers-a-data-driven-approach/>
- [28] Lewandowsky, S., & Pomerantsev, P. (2022). Technology and democracy: A paradox wrapped in a contradiction inside an irony. *Memory, mind & media*, 1, e5. <https://www.cambridge.org/core/journals/memory-mind-and-media/article/technology-and-democracy-a-paradox-wrapped-in-a-contradiction-inside-an-irony/F904B05B7ECC05A844E8E4EA7F86DC0>
- [29] Lewandowsky, S., & Van Der Linden, S. (2021). Countering misinformation and fake news through inoculation and prebunking. *European review of social psychology*, 32(2), 348-384. <https://www.tandfonline.com/doi/abs/10.1080/10463283.2021.1876983>
- [30] Minici, M., Luceri, L., Cinus, F., & Ferrara, E. (2024). Uncovering coordinated cross-platform information operations threatening the integrity of the 2024 US presidential election online discussion. *arXiv preprint arXiv:2409.15402*. <https://arxiv.org/abs/2409.15402>
- [31] Nguyen, D., Astrid, M., Kacem, A., Ghorbel, E., & Aouada, D. (2025, October). Vulnerability-aware spatio-temporal learning for generalizable deepfake video detection. In *2025 IEEE/CVF International Conference on Computer Vision (ICCV)* (pp. 10786-10796). IEEE. <https://ieeexplore.ieee.org/abstract/document/11445285/>
- [32] Nguyen, T. T., Nguyen, Q. V. H., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., ... & Nguyen, C. M. (2022). Deep learning for deepfakes creation and detection: A survey. *Computer Vision and Image Understanding*, 223, 103525. <https://www.sciencedirect.com/science/article/pii/S1077314222001114>
- [33] Nyhan, B., Porter, E., Reifler, J., & Wood, T. J. (2020). Taking fact-checks literally but not seriously? The effects of journalistic fact-checking on factual beliefs and candidate favorability. *Political behavior*, 42(3), 939-960. <https://link.springer.com/article/10.1007/s11109-019-09528-x>

- [34] Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in cognitive sciences*, 25(5), 388-402. [https://www.cell.com/trends/cognitivesciences/fulltext/S1364-6613\(21\)00051-6](https://www.cell.com/trends/cognitivesciences/fulltext/S1364-6613(21)00051-6)
- [35] Porter, E., & Wood, T. J. (2021). The global effectiveness of fact-checking: Evidence from simultaneous experiments in Argentina, Nigeria, South Africa, and the United Kingdom. *Proceedings of the National Academy of Sciences*, 118(37), e2104235118. <https://www.pnas.org/doi/abs/10.1073/pnas.2104235118>
- [36] Radesky, J., Bridgewater, E., Black, S., O'Neil, A., Sun, Y., Schaller, A., ... & Campbell, S. W. (2024). Algorithmic content recommendations on a video-sharing platform used by children. *JAMA Network Open*, 7(5), e2413855. <https://jamanetwork.com/journals/jamanetworkopen/article-abstract/2819134>
- [37] Rana, M. S., Nobil, M. N., Murali, B., & Sung, A. H. (2022). Deepfake detection: A systematic literature review. *IEEE access*, 10, 25494-25513. <https://ieeexplore.ieee.org/abstract/document/9721302/>
- [38] Roozenbeek, J., Maertens, R., McClanahan, W., & Van Der Linden, S. (2021). Disentangling item and testing effects in inoculation research on online misinformation: Solomon revisited. *Educational and psychological measurement*, 81(2), 340-362. <https://journals.sagepub.com/doi/abs/10.1177/0013164420940378>
- [39] Simchon, A., Edwards, M., Lewandowsky, S., & Ognyanova, K. (2024). The persuasive effects of political microtargeting in the age of generative artificial intelligence. *PNAS nexus*, 3(2), pgae035. <https://www.pnas.org/doi/full/10.1093/pnasnexus/pgae035>
- [40] Umbach, R., Henry, N., Beard, G. F., & Berryessa, C. M. (2024, May). Non-consensual synthetic intimate imagery: Prevalence, attitudes, and knowledge in 10 countries. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1-20). <https://dl.acm.org/doi/abs/10.1145/3613904.3642382>
- [41] Walter, N., Cohen, J., Holbert, R. L., & Morag, Y. (2020). Fact-checking: A meta-analysis of what works and for whom. *Political communication*, 37(3), 350-375. <https://www.tandfonline.com/doi/abs/10.1080/10584609.2019.1668894>