

Digital Algorithms, Mis/Disinformation, and Elections in Nepal

A Study of the Legal and Algorithmic
Framework of 2022 Elections



ABSTRACT

This paper examines the role of digital algorithms in amplifying election-related mis/disinformation during Nepal's 2022 elections and assesses the adequacy of Nepal's legal response. As political communication increasingly shifts to social media, digital algorithms shape voters' perceptions in ways that may distort electoral decision-making. Using secondary data approaches, the study combines descriptive analysis of survey data with qualitative case studies of mis/disinformation found on Facebook. The paper also looks at the legislative and statutory frameworks within Nepal to tackle mis/disinformation in the election period. It further puts forth recommendations on the regulatory and structural reforms necessary to strengthen Nepal's institutional capacity to address election-related disinformation. In doing so, the study aims to contribute to ongoing discussions on safeguarding electoral integrity in an increasingly digital political environment.

TABLE OF CONTENTS

TABLE OF CONTENTS	3
I. INTRODUCTION	4
II. METHODOLOGY	5
III. UNDERSTANDING ALGORITHMS	6
A. The Nature of Attention Algorithms	6
B. The Architecture of Recommendation Algorithms	6
IV. ELECTION MISINFORMATION ECOSYSTEM IN NEPAL	9
A. Misinformation Management During Elections in Nepal	11
i. Algorithmic Governance and Low-Resource Languages	11
ii. Maintaining Election Integrity Together	13
B. Emergence of Algorithmic Manipulation in Nepal	14
C. Case Studies from the 2022 Elections	15
V. REGULATORY AND LEGAL FRAMEWORKS IN NEPAL	18
A. Electronic Transaction Act 2063	18
B. Directive for Regulating the Use of Social Media Platforms 2080	19
C. National Penal Code 2074	21
D. Electoral Code of Conduct	21
E. Constitutional Tensions	22
F. Enforcement Challenges	23
VI. RECOMMENDATIONS	25
VII. CONCLUSION	29

I. INTRODUCTION

In today's digital age, a large share of political information is consumed through online platforms. Whilst this ensures easy access to information for voters, concerns arise about the spread of false and misleading information. The use of social media algorithms and access to Generative AI can be severely disruptive to the election process. Malicious use of social media algorithms can sway the perception of voters, inciting aggression and distorting voter sentiments. Such content can deliberately manipulate voters by appealing to anger, fear, or bias, exploiting emotions to sway decisions, create confusion, or polarise opinions in favour of particular candidates or parties. This, ultimately, undermines informed decision-making in a democracy, weakens public trust in the electoral institutions, and tilts the political playing field unfairly.

Through this paper, we aim to answer the research question: How do digital algorithms work to spread mis/disinformation during elections, and how do Nepali legal frameworks address it?

Case studies of Nepal's general elections in 2022 have been used as references, as it was the first instance where visible impacts of algorithm-boosted election campaigns were observed in mainstream politics in Nepal. In the paper, the Nepali legal and regulatory frameworks have been interpreted to show the most relevant provisions to tackle the aforementioned issue, and recommendations have been drawn from the comparative analysis with Indian frameworks, coupled with the insights of cyber law experts.

II. METHODOLOGY

This paper adopts an informative research design to investigate the role of digital algorithms in spreading misinformation during Nepal's elections. It specifically looks into the case study of the 2022 general elections, as this trend was observed first-hand by the authors in 2022. This paper also evaluates the legal and regulatory frameworks addressing the aforementioned issues.

A secondary data collection approach has been employed to reach the findings, combining both qualitative and quantitative methods. The qualitative component includes case studies, cyber lawyers' insights, and analysis of laws.

Insights from Key Informant Interviews with two cyber lawyers have been used to complement the paper and draw recommendations for Nepal to efficiently regulate online mis/disinformation during elections. The limitation of this paper is that the internal workings of platform algorithms are not publicly accessible, so this research examines and draws inferences from observations.

Key Informants provided informed consent, and participation was entirely voluntary. These findings have been reported objectively, without any political bias, and are intended solely to inform understanding of algorithmic influence and regulatory challenges.

III. UNDERSTANDING ALGORITHMS

A. The Nature of Attention Algorithms

The nature of algorithms and the mechanisms by which misinformation might spread are still opaque for most social media applications we use today. Platforms additionally may leverage perceptions of their epistemic authority on their algorithms to undermine users' confidence in what they know about algorithms and destabilize credible criticism.¹ However, we can generally assume what algorithms do thanks to some open-source implementations, whistleblower reports and information gathered about algorithms over time to study how they promote misinformation.

B. The Architecture of Recommendation Algorithms

Most modern content-delivering algorithms (like Facebook, Instagram, TikTok) function as “funnels” that personalize content from big pools to curate what the user sees². On Instagram, the “Explore” page is one of the largest recommendation systems in the application, which manages content delivery in a distinct 4-step process: retrieval, first-stage ranking, second-stage ranking and the final reranking.

During this process, the system has a preference for content historically aligned with the user's preferences and for trending content. To determine what content reaches the user, Meta utilizes a formula known as the value model (VM), which weighs different probabilities of interactivity:

Expected Value = $W_{\text{click}} * P(\text{click}) + W_{\text{like}} * P(\text{like}) - W_{\text{see_less}} * P(\text{see less}) + \text{etc.}$

¹ Cotter, K. (2023). “Shadowbanning is not a thing”: Black box gaslighting and the power to independently know and credibly critique algorithms. *Information, Communication & Society*, 26(6), 1226–1243. <https://doi.org/10.1080/1369118X.2021.1994624>

² Meta Engineering. (2023, August 9). *Scaling the Instagram Explore recommendations system - Engineering at Meta*. <https://engineering.fb.com/2023/08/09/ml-applications/scaling-instagram-explore-recommendations-system/>

This specific formula is deployed during the second-stage ranking phase. After initial retrieval algorithms narrow down millions of media contents to a shortlist of hundreds, a complex neural network computes individual probability vectors (P) for various user actions based on the user's interaction history.

The values in place of (W) serve as tunable “volume knobs” for engineers who focus on aligning algorithmic output to strike a balance between the user's interests and the platform's priorities. For instance, engineers in Meta can use a higher W-like weight, which will align the value model to pay more attention towards providing the user with posts that they might end up liking.

Meta can tune hundreds of parameters that control the behavior of the system. The engineers have control over which content pool to prioritize, how many posts to take from a particular source, how many items to select before the second stage, and the hundreds of metrics in the value model, which allows them to meticulously align the model to fit Meta's priorities at any given time.

However, engagement-based rankings optimise content for revealed preferences, which incite impulsive clicks and promote dwelling, rather than provide content that users value.³ In 2017, Meta introduced the “Meaningful Social Interactions” (MSI) update, which rewarded user interactions in the community by predicting posts Meta thought the user may want to interact with their friends about and by showing them these posts higher in the feed.⁴ The downside to this approach was that posts that sparked the most interactions tended to be the ones that made people

³ Milli, S., Carroll, M., Wang, Y., Park, S., Zhang, S., & Dragan, A. D. (2025). *Engagement, user satisfaction, and the amplification of divisive content on social media*. PNAS Nexus, 4(3). <https://doi.org/10.1093/pnasnexus/pgaf062>

⁴ Mosseri, A. (2018, January 11). *News Feed FYI: Bringing people closer together*. Meta. <https://about.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together>

offended or angry.⁵ Additionally, over the next 3 years, Meta would support posts that users reacted “angry” to, weighing them five times more valuable than likes.⁶ At this time, Facebook was effectively supporting the spread of misinformation, disinformation and divisive content through their MSI algorithm.

In this way, engagement-based recommendation algorithms permit misinformation to enter the pool and get viral by mistaking polarization for interactivity.

⁵ Oremus, W., Alcantara, C., Merrill, J. B., & Galocha, A. (2021, October 26). *How Facebook’s algorithm works*. The Washington Post.

<https://www.washingtonpost.com/technology/interactive/2021/how-facebook-algorithm-works>

⁶ Merrill, J. B., & Oremus, W. (2021, October 26). *Five points for anger, one for a “like”: How Facebook’s formula fostered rage and misinformation*. The Washington Post.

<https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm>

IV. ELECTION MISINFORMATION ECOSYSTEM IN NEPAL

As discussed, Meta has control over hundreds of changeable weights and parameters in their content delivery mechanism and, consequently, in misinformation control. Exercising this, from November 2020 to March 2021, Meta allegedly carried out 63 news feed changes in the US elections. Out of which, at a certain point in time, misinformation from untrustworthy news outlets saw a decrease in exposure up to 24%.⁷ Regionally close to Nepal, in 2019, Meta announced it was deploying artificial intelligence to clean up its platform from misinformation in India, warning India's political parties against spreading politically motivated spam messages on WhatsApp.⁸

Meta executives define these situations as “break-glass measures” during an emergency to prevent civil unrest and violence from erupting.⁹ However, it should also be pointed out that Meta rolled back to its pre-election configuration after March 2021 in the United States in the interest of market growth.¹⁰ In the case of algorithmic changes, there is an absence of a harmonized global standard where regions outside the EU lack direct, proactive and public-facing transparency rights granted, especially in a country like Nepal.¹¹ This causes users to be unaware of the drastic changes in the nature of information delivered to them.

⁷ Bagchi, C., Menczer, F., Lundquist, J., Tarafdar, M., Paik, A., & Grabowicz, P. A. (2024). *Social media algorithms can curb misinformation, but do they?* Zenodo. <https://doi.org/10.5281/zenodo.13787981>

⁸ Iyengar, R. (2021, October 29). Partisanship, employee dissent and 'dead bodies': Inside Facebook's struggle to combat misinformation and hate speech in India. *CNN*. <https://edition.cnn.com/2021/10/29/tech/facebook-india-misinformation-hate-speech>

⁹ Garrison, J., & Guynn, J. (2020, September 22). *Facebook ready in from g 'break-glass' tools to restrict content if violence erupts after election*. USA Today. <https://www.usatoday.com/story/news/politics/elections/2020/09/22/election-2020-facebook-has-break-glass-measures-if-violence-erupts/5866803002/>

¹⁰ Bagchi, C., Menczer, F., Lundquist, J., Tarafdar, M., Paik, A., & Grabowicz, P. A. (2024). *Social media algorithms can curb misinformation, but do they?* Zenodo. <https://doi.org/10.5281/zenodo.13787981>

¹¹ European Commission. (n.d.). *How the Digital Services Act enhances transparency online*. Shaping Europe's Digital Future. <https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency>

While the European Union enforces strict, public-facing audit mandates under their Digital Services Act and the United Kingdom's Online Safety Act requires regulatory reporting, the vast majority of jurisdictions outside the EU lack legally binding mandates that require platforms to proactively disclose real-time shifts in algorithmic patterns.

Professor Paik of University College Dublin (UCD) said, "Our results show that social media companies can mitigate the spread of misinformation by modifying their algorithms but may not have financial incentives to do so", in a report where he discusses the publication "Social media algorithms can curb misinformation, but do they?"¹². The engagement model was designed for entertainment and not information.¹³ The business model nudges content creators to produce highly engaging content, which users will see, interact with, comment on, and share with their network. Since highly engaging content is often emotional and controversial, content creators lean toward polarizing opinions as they gather more reposts, comments, and shares. The creators also have financial incentives to do so as the revenue model for creators rewards high engagement numbers in clicks, views, comment depth and shares.¹⁴ Within this structure, polarizing content is highly profitable while being cheap to manufacture. Misinformation is a subset of polarizing content, whose reach is supercharged by the audience engaging with it.¹⁵

¹² University College Dublin. (2024, September 27). *New eLetter in Science debunks Meta-funded study suggesting its news-feed algorithms are not major drivers of misinformation*. UCD News. <https://www.ucd.ie/newsandopinion/news/2024/september/27/neweletterinsciencedebunksmeta-fundedstudysuggestingitsnews-feedalgorithmsarenotmajordriversofmisinformation/>

¹³ Diaz Ruiz, C. (2023). Disinformation on demand: How digital markets drive the production of low-quality information. *New Media & Society*. Advance online publication. <https://doi.org/10.1177/14614448231207644>

¹⁴ Bakir, V., & McStay, A. (2018). Fake news and the economy of emotions: Problems, causes, solutions. *Digital Journalism*, 6(2), 154–175. <https://doi.org/10.1080/21670811.2017.1345645>

¹⁵ Annenberg School for Communication. (2024, June 5). *New study uncovers how information spread on Facebook in the lead up to and after the 2020 election*. University of Pennsylvania. <https://www.asc.upenn.edu/news-events/news/new-study-uncovers-how-information-spread-facebook-lead-and-after-2020-election>

A. Misinformation Management During Elections in Nepal

i. Algorithmic Governance and Low-Resource Languages

Meta's automated filters and content moderators often fall short when dealing with non-English content.¹⁶ While Meta contains the spread of racial or religious hatred online in the primarily developed countries and communities where global languages like English, Spanish and Mandarin dominate, it is difficult for the rest of the world, especially for minorities, to be safe from targeted hate speech.¹⁷ Analysis by Julia High ran tests of multiple violating words in the Facebook search dialog and observed that in English, 49.1% of words triggered a pop-up deterrence message. In contrast, only 21.1% of Spanish words did.¹⁸ A pop-up deterrence message is a safety intervention on the Facebook search page which is triggered when a user inputs query parameters flagged for high risk, such as terms associated with self-harm, violent extremism or illicit commerce.¹⁹

Particularly, the algorithms, which are rooted in machine learning and natural language processing (NLP), are designed to identify content that violates "Community Standards" and particularly flag items of hate speech and disinformation, rather than misinformation, which is harder to track and subjective by nature.²⁰

¹⁶ Okong'o, J. (2025, April 9). *Meta is failing to stop dangerous disinformation in the world's most spoken languages*. Poynter. <https://www.poynter.org/fact-checking/2025/meta-disinformation-non-english-languages/>

¹⁷ Perrigo, B. (2019, November 26). *Facebook says it's removing more hate speech than ever before. But there's a catch*. Time. <https://time.com/5739688/facebook-hate-speech-languages/>

¹⁸ High, J. (2025, February 25). *Facebook's search interventions: Bad in English, Peor en Español*. Technology Science. <https://techscience.org/a/2025022503self-harm/>

¹⁹ Perrigo, B. (2019, November 26). *Facebook says it's removing more hate speech than ever before. But there's a catch*. Time. <https://time.com/5739688/facebook-hate-speech-languages/>

²⁰ Anti-Defamation League, Avaaz, Decode Democracy, Mozilla, & New America's Open Technology Institute. (n.d.). *Content moderation*. Mozilla Foundation. <https://www.mozillafoundation.org/en/campaigns/trained-for-deception-how-artificial-intelligence-fuels-online-disinformation/content-moderation/>

Furthermore, the automation gap is hardly corrected by human oversight. Third-party content moderation vendors assigned to a region are usually under-resourced and under stringent quota-driven time constraints.²¹ Specifically, in the case of a low-resource language like Nepali, a handful of people would be responsible for millions of active users. The platform cannot assure control over the containment of misinformation in the region in this scenario. This risks the chances of a highly volatile spread of misinformed narratives across the Nepali ecosystem.

In disinformation control as well, Meta's algorithm in Nepal is hindered by the Nepali language being "romanized" and the prevalence of "code-switching" –intermixing of Nepali and English in online discourse.²² Research on bilingual fake-news detection in Nepal suggests modern transformer-based models can achieve high accuracy in set environments, but their performance drops by up to 7% when dealing with heavy code-mixing and informal slang.²³ This gap creates opportunities for harmful/misinformed content to spread using localised slang and non-standard code-switching.

Additionally, the problem is difficult to understand and solve for regional languages like Maithili and Bhojपुरi. These languages are still prevalent in politically sensitive Terai, but are categorized as low-resource languages with minimal data to train models. Internal Meta documents suggest low-resource languages are translated to English for detection,²⁴ but this action misses nuances like satire, irony or subtle threats in speech that do not translate directly into other languages.

²¹ Balendra, S. (2025). Meta's AI moderation and free speech: Ongoing challenges in the Global South. *Cambridge Forum on AI: Law and Governance*, 1. <https://doi.org/10.1017/cfl.2025.5>

²² Ghimire, P., & Shrestha, P. (2025). *Bilingual fake-news detection in low-resource media: A Transformer-based framework for Nepali-English content*. ResearchGate. <https://doi.org/10.13140/RG.2.2.33923.41767>

²³ Ghimire, P. (2025, May 29). *Evaluating the disparity in content moderation: A cross-linguistic analysis of Facebook's safety interventions* (Version 1). Research Square. <https://doi.org/10.21203/rs.3.rs-6778598/v1>

²⁴ Okong'o, J. (2025, April 9). *Meta is failing to stop dangerous disinformation in the world's most spoken languages*. Poynter. <https://www.poynter.org/fact-checking/2025/meta-disinformation-non-english-languages/>

ii. Maintaining Election Integrity Together

For the first time in 2022, the Election Commission of Nepal attempted to expand relations with social media platforms to reduce the number and impact of misinformation that could spread online during elections.²⁵ The Commission also established a monitoring unit, including the cyber bureaus of Nepal Police and Nepal Army, to monitor misinformation and hate speech transmitted through online media. Among Meta, TikTok and X (formerly known as Twitter), Meta collaborated with ECN while TikTok and X opened direct communication channels regarding election-related misinformation.

Meta helped bring transparency into election-related advertisement data from the Facebook Ad Library by publishing and archiving information on political ads like who funded them, approximate costs and their reach across multiple demographics. Additionally, Meta discussed and consulted with Election Commission officials and held a conference on ‘National Election Hygiene’ on the 18th of October 2022.²⁶

However, the ECN spokesperson Shaligram Sharma Poudel tells [NepalMinute.com](https://nepalminute.com) that they just report and request Meta and other platforms to take down the content, after which the Election Commission has no control.²⁷ Since Meta lies beyond Nepal’s jurisdiction, Poudel said they cannot enforce Nepali rules upon these platforms. Poudel added, “Social media companies don’t have

²⁵ Acharya, U. (2022, December 20). Interventions to combat misinformation in Nepal’s 2022 elections. Center for Media Research - Nepal.

<https://research.butmedia.org/interventions-to-combat-misinformation-in-nepals-2022-elections/>

²⁶ ICT Frame. (2022, October 11). *Election Commission Nepal to cooperate with Meta.*

<https://ictframe.com/election-commission-nepal-cooperate-with-meta/>

²⁷ Ghimire, D. (2022, November 11). *Election body red flags online contents that violate poll code.*

<https://www.nepalminute.com/detail/1048/election-body-red-flags-online-contents-that-violate-poll-code>

offices in Nepal, nor do the government agencies have established ties with these companies. That makes it difficult to enforce these rules.”

In Nepal, Meta and X have consistently ignored consecutive government ultimatums, including a final compliance deadline in late 2025 that threatened platform deactivation. Representing Meta, the Asia Internet Coalition (AIC) particularly pushed back on the mandate that the company is required to arbitrarily purge flagged content within a 24-hour window, as technically unviable and non-compliant with international human rights frameworks. While Meta complies with fiscal regulations by paying digital service taxes to Nepal’s Inland Revenue Department, the refusal to establish a domestic legal entity leaves a systemic vacuum. This absence nullifies Nepal’s capacity to legally enforce localized content moderation during acute disinformation crises.²⁸

B. Emergence of Algorithmic Manipulation in Nepal

The 2022 elections saw a shift from the spontaneous spread of rumours to organized information manipulation in Nepal. Using Meta’s algorithms to shape public perception, organized “cyber forces”, particularly called “cyber sena” in Nepali contexts, were engaged to game the platform’s engagement metrics to favour partisan narratives and suppress opposition.²⁹

This coordinated effort of sharing partisan media to manipulate public debate through social media is identified by Meta as Coordinated Inauthentic Behaviour (CIB)³⁰. Cyber forces utilise networks

²⁸ Maharjan, Uttam. (2025, May 13). *Resolve Meta Registration Impasse*. The Rising Nepal. <https://risingnepaldaily.com/news/61828>

²⁹ Dahal, R., & Acharya, U. (2025). An anatomy of information manipulation in Nepal. In U. Acharya (Ed.), *Nepal's misinformation landscape* (pp. 25–49). Center for Media Research – Nepal. <https://doi.org/10.62657/cmr25a>

³⁰ Meta. (2024, October 11). *Taking action against coordinated inauthentic behavior in Moldova*. Meta Newsroom. <https://about.fb.com/news/2024/10/taking-action-against-coordinated-inauthentic-behavior-in-moldova/>

of fake accounts and partisan media outlets to engage in organized sharing. This practice ensures particular posts receive massive spikes in likes, comments and shares immediately upon publication, possibly tricking Meta’s recommendation engine into categorizing the content as “trending”, which could consequently push the content to the news feeds of thousands of unaligned voters.

In 2022, the most effective measures of spreading misinformation stemmed from screenshot sabotage, context stripping from old videos, and fake engagement from cyber forces. Screenshot sabotage and context stripping are examples of “shallow fakes”.³¹ Unlike their counterpart “deepfakes”, shallowfakes don’t use deep learning algorithms, but instead are created using easily accessible tools such as basic video, photo or audio editing software.³² Screenshots were manipulated to be believable, like forged news articles from reputed sources, and videos were stripped of context using various methods. Compared to deepfakes, the spread of misinformation proved far more effective using shallow fakes, as the videos were “real” footage, only stripped of context.

C. Case Studies from the 2022 Elections

As discussed, election-related misinformation in Nepal manifests itself through fake posts, doctored images, fabricated screenshots of news reports, and out-of-context videos.³³ A trend observed in the elections of 2022 featured most of this online mis/disinformation to be strategically edited political speeches by the politicians to reverse their original meaning.

³¹ Meta. (2022, November). *Quarterly adversarial threat report, Q2 2022*.

<https://about.fb.com/wp-content/uploads/2022/11/Quarterly-Adversarial-Threat-Report-Q2-2022-1.pdf>

³² Mea Digital Evidence Integrity. (2024, February 7). *What are shallowfakes and how do they work?*

<https://www.mea-integrity.com/what-are-shallowfakes-and-how-do-they-work/>

³³ Adhikari, D. (2022, December 13). *Doctored images and out-of-context videos spread misinformation during Nepal elections*. *OnlineKhabar English*. <https://english.onlinekhabar.com/misinformation-elections-nepal.html>;

NepalCheck. (2022, November 5). *Claims Gagan Thapa campaigned for Maoists are misleading*. <https://nepalcheck.org/2022/11/05/claims-gagan-thapa-campaigned-for-maoists-are-misleading/>

Recorded cases of election misinformation:

- A video featured Pushpa Kamal Dahal allegedly saying that elections can only be won through manipulation and ballot box swapping. Later, it was confirmed that the video was deceptively edited.³⁴
- Similarly, a video showed Gagan Thapa promising free, generous monthly allowances, free mobile phones, and fuel if he became the PM. In reality, he was actually saying how it has been easy to make populist promises and how difficult it is to fund them.³⁵
- Likewise, a video displayed CPN-UML leader Pradeep Gyawali encouraging the spread of confusion during elections, when he was only responding sarcastically to allegations by rival factions.³⁶
- Further, a fake screenshot in 2022 held that Rabi Lamichhane had entered into an electoral alliance with CPN-UML, and many voters accepted the claim until this was later disproved.³⁷

These false and misleading news were strategically circulated to sway voters' perception before the elections. This news creates confusion, emotional reaction, and distrust during a politically sensitive period. Much of this manipulated content relied on pre-existing public perceptions of politicians. For instance, populist narratives attached to Gagan Thapa's clip resonated with the public because they aligned with public frustration regarding unrealistic electoral promises. Similarly, allegations of manipulation involving Pushpa Kamal Dahal gained traction due to

³⁴ Shrestha, U. (2022, December 23). निर्वाचनमा फैलिएका मिथ्या सूचना [Misinformation spread during elections]. *Ekantipur*. <https://ekantipur.com/opinion/2022/12/23/167175931594428802.html>

³⁵ *ibid*

³⁶ *ibid*

³⁷ Nepal Factcheck. (2023, April). रास्वपाले तनहुँमा एमालेलाई सघाउने दावी गरिएको स्क्रिनसट नक्कली [Fact check: Screenshot claiming RSP helped UML in Tanahun is fake]. *NepalFactCheck.org*. <https://nepalfactcheck.org/2023/04/rsp-fake-screenshot/>

longstanding public scepticism regarding political elites and the electoral process itself. The likely objective of this type of content was not only to damage the reputations of individual candidates but also to shape voter perception through doubt, cynicism, and emotional polarization. Even when this news was later disproved, misleading narratives may also have already influenced public discussions and reinforced biases. Assessing the actual electoral impact of these manipulation efforts remains difficult due to the absence of empirical data on voter behaviour and digital influence in Nepal. However, it is reasonable to deduce that repeated exposure to manipulated political content risks normalizing distrust in institutions, weakening informed political participation and reducing citizens' ability to distinguish between legitimate criticisms and fabricated notions.

V. REGULATORY AND LEGAL FRAMEWORKS IN NEPAL

The following section examines the legal and institutional mechanisms available in Nepal to regulate election-related mis/disinformation.

A. Electronic Transaction Act 2063

The Electronic Transaction Act, 2063, stipulates in its preamble that it aims to regulate electronic communication reliably and securely. Mis/Disinformation challenges the very reliability of electronic communication. To regulate such activities, the primary statutory response exists in Section 47 of the Act, which criminalizes the publication and dissemination of electronic content deemed ‘contrary to public morality’ or ‘that may jeopardize harmonious relations’ with up to 5 years’ imprisonment or a fine of Rs 100,000. In electoral contexts, this provision can be interpreted against online misinformation and defamatory political content.

The ETA mentions in Section 43 that no network service providers shall be liable to bear any civil or criminal liability arising from the dissemination of information by third-party users. Third-party users in this context signal the users (the provision explicitly refers to third-party users as the person over whom there is no control of the network service providers). Whilst Facebook might not seem like a network service provider in the literal manner, it can be interpreted to be one through the purposive interpretation of a law. Section 43 aims to protect intermediaries that provide access to third-party electronic information without control over its content. Facebook fits this intermediary role and should be included. Hence, Facebook has a safe harbour immunity whereby it isn’t penalized for the mis/disinformation circulated by its users. However, the immunity provided to the network service providers is not absolute, and this immunity may be lost where the

intermediary possesses knowledge of the unlawful nature of the content and continues to facilitate access.

B. Directive for Regulating the Use of Social Media Platforms 2080

It is worth noting that this immunity-based framework is further complicated by the Directive for Regulating the Use of Social Media Platforms, 2080. The Directive signals a shift toward greater platform accountability and defines social networks broadly as platforms that enable interactive communication and user-generated content through electronic means. Unlike the ETA, which treats the intermediaries as passive hosts, the Directive places an obligation on platform operators to actively regulate content. Section 4 of the Directive explicitly prohibits the publication and dissemination of false information, misleading information, and disinformation.³⁸ Section 8 further requires platforms to adopt algorithmic and technical measures to prevent unlawful content from being published or circulated.³⁹

Further, the Directive also requires platforms to remove prohibited content within twenty-four hours of receiving complaints or official instructions, establish grievance-handling mechanisms, and verify the accuracy of content circulating on their platform.⁴⁰ Hence, the Directive reflects how social media is now seen as an active actor with regulatory responsibilities over online content.

In saying so, the question of whether Facebook is liable to adhere to Nepali laws is bound to arise. The effects doctrine in cyber law provides that a country may exercise jurisdiction over actions that occur outside its territory if those actions produce substantial effects within its borders. As has been

³⁸ Directive for Regulating the Use of Social Media Platform, 2080, § 4

³⁹ Directive for Regulating the Use of Social Media Platform, 2080, § 8

⁴⁰ *ibid*

upheld in the case of *LICRA v. Twitter*, foreign platforms accessible in a country and operating services that affect users there can be required to comply with that country's statutory obligations, even if not incorporated locally.⁴¹ While *LICRA v Twitter* is not binding in Nepal, it provides us with a persuasive comparative reasoning for understanding how states could seek to impose legal obligations upon foreign digital platforms whose services produce effects within their territory. On this same basis, it may be argued that Facebook is expected to comply with Nepal's regulatory framework. In practice, however, enforcement against foreign platforms such as Facebook remains difficult because user data, account records, and digital evidence are stored outside Nepal. Meta's policies themselves state that the disclosure of account information requires a Mutual Legal Assistance Treaty (MLAT) or letters rogatory.⁴² Hence, where Nepali authorities try to identify the people behind defamatory or misleading election-related content, cooperation from foreign jurisdictions and the platform itself becomes necessary. And it cannot be overlooked that platforms such as Facebook also operate through their own internal reporting, complaint, and content moderation systems, such that regulation of online mis/disinformation is not only shaped by domestic law but also by platform-governance mechanisms operating across jurisdictions.

Meta's Community Standards themselves recognise voter interference, manipulated media, and misleading electoral content as categories that require moderation.⁴³ The policies of the platform provide removal, labelling, reduced distribution, and fact-checking of such content. This affirms

⁴¹ UEJF v. Twitter. (n.d.). In *Global Freedom of Expression* | Columbia University. Retrieved February 3, 2026, from <https://globalfreedomofexpression.columbia.edu/cases/uejf-v-twitter/>

⁴² Meta Platforms, Inc. *What happens to your content when you report it on Facebook*. Facebook Help Center. <https://www.facebook.com/help/494561080557017>

⁴³Meta Platforms, Inc. (n.d.). *Misinformation*. Meta Transparency Center. <https://transparency.meta.com/policies/community-standards/misinformation/>

that social media platforms increasingly exercise quasi-regulatory functions in managing election-related mis/disinformation.

C. National Penal Code 2074

Certain forms of election-related mis/disinformation may also intersect with criminal liability under section 306 of the National Penal Code, 2074, relating to defamation.⁴⁴ This provision explicitly criminalizes the publication or dissemination of imputations that harm another person's reputation, including through words, signs, or visual representations. In electoral contexts, manipulated speeches, fabricated screenshots, or misleading content targeting political candidates may potentially fall within this scope as they are likely to be circulated with knowledge or intent to damage reputation, especially in politically sensitive periods.

D. Electoral Code of Conduct

Further, the Election Commission Act, 2073, grants the Election Commission the power to issue a code of conduct during the election. Based on this statutory power, the Election Code of Conduct, 2022, in Section 4, prohibited transmission of disinformation, misinformation, and hate speech in social networks.⁴⁵ This Code is applicable as it was the governing Code for the elections in 2022. The same Code of Conduct has defined disinformation to be the act of communicating false or misleading information knowingly with the intention of making an advantage to oneself and causing harm to others, with the intention of misleading the public. However, it also excuses honest mistakes arising while reporting about the election from being termed as misinformation.

⁴⁴ National Penal Code, 2017, §306

⁴⁵ Election Commission Act, 2073, § 4

Section 3 of the Code of Conduct expresses that the code will apply to private and non-governmental organisations, their officials and employees.⁴⁶ Private organizations are hence interpreted to affirm that social media platforms are prohibited from transmitting disinformation and misinformation on their platform.

Moreover, the code in its Section 25 prohibited communication platforms within social media from publishing and broadcasting false and misleading news harming candidates and their families' dignity.⁴⁷ News portals within social media platforms have been prone to circulating such content, as has been evident from the examples above. Further, the code in the same section prohibited the transmission of comments on the internet that spread misinformation and disinformation with the intention to influence the elections. These legal provisions could have been directly applied in the instances of 2022. It is also important to note that the Supreme Court itself ruled in 2024 that editors and publishers have a duty to verify the accuracy of sensitive content before dissemination. Hence, the media rooted in social media platforms have a big role in ensuring the aforementioned.⁴⁸

E. Constitutional Tensions

Back in 2022, the Election Commission had ordered the removal of a social media page, 'No Not Again', claiming it defamed candidates. It had also filed a complaint at the Nepal Police's Cyber Bureau to take action against the page through the ETA, 2063.⁴⁹ However, 'No Not Again' merely informed voters about the right to reject candidates who had once become prime ministers and had

⁴⁶ Election Code of Conduct, 2022, § 3

⁴⁷ Election Code of Conduct, 2022, § 25

⁴⁸ Dulal, D. (2024, September 30). *Sidhakura case: SC ruling sets precedent on media contempt and freedom of expression*. Ratopati English. <https://english.ratopati.com/story/35157/>

⁴⁹ OnlineKhabar English. (2022, November 6). *Supreme Court: Don't take action against No Not Again*. <https://english.onlinekhabar.com/supreme-court-for-no-not-again.html>; Kathmandu Post. (2022, November 6). *Supreme Court issues interim order in favour of 'No Not Again' campaign*. <https://kathmandupost.com/national/2022/11/06/supreme-court-issues-interlocutory-interim-order-not-to-take-action-against-no-not-again-campaigners>

yet failed to perform. The Supreme Court issued an interlocutory order against the Election Commission to not take action against the campaigners of the ‘No Not Again’ movement. This case demonstrates the lack of a clear distinction between political criticism and misinformation, which further creates a conflict with fundamental rights.

The Constitution of Nepal, 2072, in its Article 17, guarantees the freedom of expression to a person and prosecution arising out of political criticism violates one’s fundamental right. The European Court of Human Rights in the case of *Lingens v. Austria* ruled that the conviction of a journalist for criticizing a politician violated freedom of expression, and that political figures must tolerate a higher degree of criticism because political speech on matters of public interest receives strong protection.⁵⁰ This landmark case can be taken as an important principle to look into the ‘No Not Again’ case.

F. Enforcement Challenges

It is important to distinguish election-related mis/disinformation from other forms of online harm already prosecuted under existing cyber laws. Section 47 of the ETA has been invoked in cases involving obscenity, harassment, revenge pornography, and other forms of direct online abuse where harm is relatively identifiable and immediate.⁵¹ Election-related mis/disinformation operates differently, unlike, say, revenge pornography or explicit online harassment, as misinformation often involves questions of political speech, public discourse, satire, and manipulation. The harm caused is not always directed towards an individual alone, but may extend to electoral integrity, democratic participation, and public trust. Applying the same broad legal standard to fundamentally different

⁵⁰ *Lingens v. Austria*, Application No. 9815/82, European Court of Human Rights (1986). *Global Freedom of Expression* | Columbia University. <https://globalfreedomofexpression.columbia.edu/cases/lingens-v-austria/>

⁵¹ Ojha, A. (2023, February 9). *The troubling rise of ‘revenge porn’ in Nepal*. The Kathmandu Post. <https://kathmandupost.com/national/2023/02/09/the-troubling-rise-of-revenge-porn-in-nepal>

forms of online harm can risk inconsistency with the application of doctrines and raise concerns about overcriminalisation and suppression of legitimate political expression.

These conceptual difficulties are further reflected in the practical enforcement of Nepal's existing legal framework. Whilst interpretation can be drawn from the existing legal provisions to regulate election-related mis/disinformation in social media, three major problems prevent legal provisions from operating efficiently. Firstly, the laws are too vague and are misused to silence legitimate criticism. This is evident from the case of 'No Not Again'. Also, laws should be applied consistently with the mischief they were enacted to prevent. Over-reliance on Section 47 stretches the provision beyond its legislative purpose and creates doctrinal misuse.

Secondly, enforcement is selective and inconsistent. This is evident by the fact that Chief EC Commissioner Thapaliya publicly admitted that government officials themselves spread false information, like Madhesh CM, who used photos of Delhi to show development in his province. Yet, no actions were taken.⁵²

Third, our regulatory framework is currently struggling to keep pace with digital realities. The Cyber Bureau's reactive, complaint-based mandate prevents timely intervention, and the extraterritorial status of major platforms also hinders enforcement, allowing mis/disinformation to operate with near-total impunity.

⁵² Dahal, R., & Acharya, U. (2025). *An anatomy of information manipulation in Nepal*. In U. Acharya (Ed.), *Nepal's misinformation landscape* (pp. 25–50). Center for Media Research – Nepal. https://research.butmedia.org/wp-content/uploads/2025/03/NML_Anatomy_of_Misinformation_Rishikesh_Dahal_Ujjwal_Acharya.pdf

VI. RECOMMENDATIONS

The 2022 elections revealed structural weaknesses in Nepal's regulations pertaining to election-related mis/disinformation. Some legal provisions indeed existed; however, their application and implementation remained largely inconsistent, and their scope was also unclear. Addressing election-related mis/disinformation requires strong enforcement of existing mechanisms and reforms that address emerging digital challenges.

In the short term, Nepal must assert its existing regulatory frameworks properly. The Election Commission of Nepal should enforce its Code of Conduct more rigorously, specifically in cases involving hate speech and racially or sexually charged disinformation. Cyber lawyer Adv. Abhinawa Khakurel notes that when candidates deliberately disseminate harmful content, the Commission must be willing to impose serious deterrence measures, even extending to the disqualification of their candidacy. Such serious punishments can largely make people think twice before posting such false or misleading information. He also emphasises that penalties must be proportionate to the offender's financial capacity and institutional position, especially where public officials or influential actors are involved.

At the same time, clear legislative frameworks must exist to prevent misuse of existing laws. Nepal's cyber regulatory framework relies heavily on broadly worded provisions, particularly under the Electronic Transaction Act, 2063. These provisions were not designed primarily to address election-related disinformation and misinformation, and therefore require extensive interpretation. Legislative reforms must be based on clear, Act-based definitions of electoral disinformation that distinguish between deliberate manipulation, honest reporting errors, and legitimate political

criticism, as a cyber law lecturer and lawyer, Adv. Anoushka Pant observes that current laws often focus broadly on national security and public welfare only, but election-related laws require more specific, harm-based legislation that directly addresses their impact on democratic processes and voter perception.

Another important reform that must be addressed is the nature of penalties. Minor fines or punishment often fail to deter political actors who benefit from the rapid spread of misleading political content. Advocate Pant stresses that laws must move beyond these mere sanctions to meaningfully protect electoral integrity. She mentions that disinformation must have more serious consequences than misinformation because the intent behind it is fundamentally different. Misinformation is shared without the intent to deceive; however, disinformation arises from a deliberate intention to deceive and the circulation of false information to gain a political advantage.

The role of digital platforms is also instrumental in the regulation of mis/disinformation. During the 2022 elections, Nepal's engagement with major platforms like Meta and TikTok remained informal and reactive. In contrast, countries such as India have institutionalised cooperation between election authorities and social media platforms during the election periods.⁵³ Ahead of India's 2019 general elections, major social media platforms like Facebook, WhatsApp, Twitter, and Google adopted a voluntary code of ethics in consultation with the ECI. This code emphasized transparency of political content, rapid content flagging of election-related misinformation, disinformation, and violations of the Code of Conduct, including misleading political

⁵³ Sk, S., & Pavan, T. (2024). *Regulating the fake news on social media platforms: Analyzing the impact of Indian legal system and legal system of other countries*. *International Journal for Multidisciplinary Research (IJFMR)*, 6(6). <https://www.ijfmr.com/papers/2024/6/31548.pdf>

advertisements and false claims about candidates, and timely grievance redressal. Such steps must also be initiated by Nepal, and the institutionalization of these steps must be done.

At the platform level, legal frameworks must establish clearer expectations regarding content moderation. Social media companies should be legally obligated to take reasonable steps to limit the spread of harmful electoral disinformation during sensitive election periods. However, this obligation should be balanced with protections against excessive censorship. Advocate Pant mentions that clear state guidelines must exist so that platforms understand the limits of acceptable moderation while also protecting legitimate political expression. For that, she adds that local focal/contact persons must exist for social media platforms so that they can help facilitate communication with regulatory authorities, respond to complaints in a timely manner, and better understand the local political and cultural context in which such content circulates. This is similar to the approach taken by India. Under India's intermediary regulatory framework, platforms are required to appoint a Chief Compliance Officer, a Nodal Contact Person, and a Resident Grievance Officer, and they must be citizens of India. These officers serve as direct points of accountability and coordination with regulatory authorities. Further, platforms are required to publish monthly compliance reports detailing the number of user complaints received, the nature of those complaints, and the actions taken in response.⁵⁴

Emerging technologies like AI further complicate the authenticity of the information. The strategic editing of political speeches observed during the 2022 elections already demonstrates how manipulated media can alter public perception. Advocate Pant highlights that Nepal should

⁵⁴ Dehradun Law Review. (2024). *[Social Media and Its Impact on the Electoral Process in India: A Critical Study]*. Dehradun Law Review, 16(1). <https://www.dehradunlawreview.com/wp-content/uploads/2025/03/10.pdf>

consider introducing legal requirements for the labelling or disclosure of AI-generated political content, especially during election periods. Such disclosure mechanisms would allow voters to better assess the credibility of the information being circulated.

Institutionally, Nepal can also benefit from strong coordination between regulatory and enforcement bodies. Enforcement still largely depends on complaint-based mechanisms, which often respond only after misleading content has been circulated widely. Establishing a dedicated election-focused cyber response mechanism could improve early detection and response. Such a unit could operate under the Election Commission and coordinate directly with the Cyber Bureau and social media platforms to verify manipulated content and flag violations more rapidly.

Beyond institutional reform, public awareness is very important, as laws alone cannot fully address the scale and speed of online mis/disinformation. Digital literacy initiatives help citizens identify manipulated content and verify information and are therefore an important preventive tool. Advocates Khakurel and Pant both mention the ripple effect of digital literacy that can sometimes be more efficient than laws, which usually take a longer time to guarantee punishments. Advocate Pant further suggests that accessible reporting mechanisms, such as free hotline numbers, could empower citizens to quickly report misleading content during election periods. Such reporting systems must be easy and quick so that citizens are actively encouraged to use them. If these reporting mechanisms are too long and tedious, one might be discouraged from opting for this measure.

Finally, Nepal's experience in the 2022 elections demonstrates that the country's current framework remains overly reliant on vague statutory provisions and reactive enforcement. A more

coherent approach would be to combine strong enforcement of the code of conduct with existing legislative provisions, cooperation with digital platforms, proportionate penalties, regulation of AI-generated content and greater digital literacy initiatives. Through these processes, electoral integrity can be better protected in future election cycles to uphold digital democracy.

VII. CONCLUSION

The 2022 elections in Nepal demonstrated the growing role of social media in facilitating the circulation of election-related mis/disinformation. Engagement-based recommendation systems often prioritise emotionally charged and polarising content. These, when combined with media distortions such as shallow fakes, can influence public discourse during elections. These technological aspects reveal how digital platforms can unintentionally facilitate the rapid spread of false and misleading political content.

While Nepal possesses certain legal and regulatory tools, their applications remain inconsistent, and their scope often remains unclear. At the same time, efforts to regulate online content must be balanced with constitutional guarantees of freedom of expression, especially in democracies where criticism and debate uphold democratic participation.

The experience of the 2022 elections, therefore, highlights the need for clearer legal frameworks, stronger institutional coordination, greater cooperation with digital platforms, and improved digital literacy among citizens. Strengthening these mechanisms will be essential to protecting electoral integrity in Nepal while ensuring that regulation does not undermine the democratic freedoms it seeks to safeguard.



Body & Data

www.bodyanddata.org

[@bodyanddata](https://www.instagram.com/bodyanddata)



Facebook



Instagram



Bluesky



X

Author: Krisha Niroula & Maharshi Kattel

Developmental Editor: Monisha Choudhary

Layout: Monisha Choudhary

Published By: Body & Data

Support: Vision for Change