International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

# Laws Against Misinformation and Fake News Online: A Review

**Meher Mehra[1], Raghu Raja Mehra[2], Mohit Sood[3]**

[1]Department of Information Technology, Invictus International School, Amritsar, India
Email: *meherharveen2728[at]gmail.com*

[2]Department of Information Technology, Invictus International School, Amritsar, India
Email: *raghumehra35[at]gmail.com*

[3]Department of Information Technology, Invictus International School, Amritsar, India
Email: *mohitsood1434[at]gmail.com*

**Abstract:** ***The proliferation of misinformation, disinformation, and synthetic media on digital platforms poses significant risks to public health, democratic processes, and social cohesion. Governments and regulators worldwide have adopted a range of legal and policy responses—from transparency and liability obligations to correction orders and criminal sanctions aimed at mitigating harm while safeguarding freedom of expression. This paper reviews recent national and supranational legal frameworks, evaluates their strengths and limitations, examines existing technological and institutional mitigation methodologies, and proposes a hybrid model that integrates adaptive legal measures with technological tools and public education to create a balanced approach. The review draws on legislative texts, policy analyses, and recent case studies (including the EU Digital Services Act, the UK Online Safety Act, India's IT Rules, and Singapore's POFMA), and discusses challenges such as cross-border enforcement and emerging synthetic-media threats. The paper concludes with policy recommendations for multi-stakeholder governance, transparency, and resilience-building.***

**Keywords**: Misinformation, Fake news, Online regulations, Digital platforms, Content moderation, Freedom of expression, Cyber laws, Social media governance, Regulatory frameworks, Fact-checking. Digital Services Act; Online Safety Act; POFMA

## 1. Introduction

The digital information environment has undergone rapid expansion during the past two decades, with social media platforms, messaging applications, and user-generated content sites serving as primary sources of news and commentary for large populations. While this has democratized voice and access, it has also lowered the barriers to producing and distributing false or misleading information. Instances of misinformation during public-health emergencies, coordinated disinformation campaigns during elections, and the proliferation of synthetic media (deepfakes) have motivated widespread policy attention (Wardle & Derakhshan, 2017; WHO, 2020).

This review surveys legal responses to online misinformation, focusing on recent developments from 2019 through 2025. It evaluates: (a) the objectives and trade-offs of regulatory approaches; (b) technological and institutional methodologies; (c) comparative jurisdictional practices; and (d) a proposed hybrid framework that balances public-safety objectives with fundamental free-speech protections. The analysis draws on primary legal texts and contemporary policy commentary.

Legal systems must walk a tightrope between mitigating demonstrable harms (electoral interference, public-health risks, violence) and preserving free expression and a plural public sphere. Recent laws show three broad families of response:

1) Systemic governance of platforms (e.g., EU Digital Services Act),
2) Content-focused duties and powers (e.g., Singapore's POFMA; Germany's NetzDG), and
3) Immunity-preserving frameworks paired with sectoral carve-outs (e.g., U.S. Section 230 plus state deepfake/election rules).

## 2. Literature Review

Scholarly literature on misinformation spans disciplines including communications, political science, law, and computer science. Research has identified cognitive drivers (confirmation bias, motivated reasoning), platform mechanics (algorithmic amplification), and actor incentives (political actors, commercial clickbait) as core contributors to information disorder (Allcott & Gentzkow, 2017; Wardle & Derakhshan, 2017). Legal scholars have debated intermediary liability, content moderation duties, and the normative limits of state intervention in speech online (Citron & Pan, 2021). International organisations such as the World Health Organization and UNESCO have emphasised multi-pronged responses combining regulation, platform practices, and public education (WHO, 2020; UNESCO, 2021).

Comparative policy analyses highlight diverging policy choices: the European Union emphasizes transparency and platform obligations (the DSA); some states (e.g., Singapore) favour statutory correction powers (POFMA); others (e.g., the United States) remain cautious about liability rules, relying instead on intermediary immunities with calls for targeted reform to Section 230 (Kosseff, 2020). Recent legal scholarship underscores the need for granular, evidence-based obligations proportionate to platform scale and function.

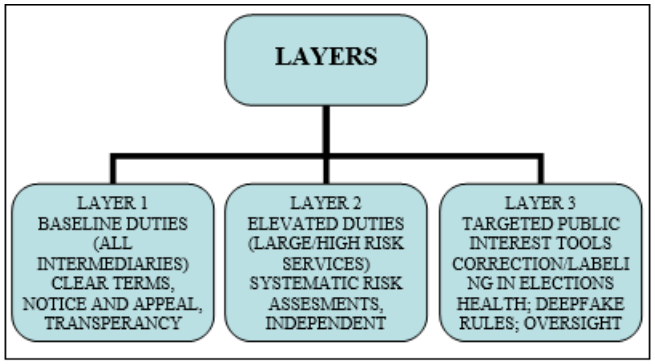


**Figure 1:** Proposed Layered Framework for Online Misinformation Laws

**Definitions**

- Misinformation: false or misleading content shared without intent to deceive.
- Disinformation: false or misleading content shared with intent to deceive.
- Malinformation: genuine content shared out of context to cause harm.

## 3. Comparative Legal Landscape

### 3.1 European Union – Digital Services Act (DSA)

The DSA introduced a tiered regime for intermediaries with the heaviest duties on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). Core obligations include risk assessments for systemic risks (including disinformation), independent audits, transparency reporting, data access for vetted researchers, and crisis protocols. Enforcement by the European Commission has advanced to formal investigations and potential penalties (reportedly first penalties targeting X).

**Table 1.** New obligations for gatekeepers in the DSA.

| | | Intermediary services | Hosting services | Online platforms | Very large online platforms |
|---|---|---|---|---|---|
| **Transparency measures for online platforms** | Transparency reporting | √ | √ | √ | √ |
| | Requirements on terms of services due account of fundamental rights | √ | √ | √ | √ |
| | Notice-and-action and obligation to provide information to users | | √ | √ | √ |
| | User-facing transparency of online advertising | | | √ | √ |
| | Transparency of recommender systems and user choice for access to information | | | | √ |
| **Oversight structure to address the complexity of the online space** | Cooperation with national authorities following orders | √ | √ | √ | √ |
| | Points of contact and, where necessary, legal representative | √ | √ | √ | √ |
| | Complainant and redress mechanism and out of court dispute settlement | | | √ | √ |
| | External risk auditing and public accountability | | | | √ |
| | Crisis response cooperation | | | | √ |
| **Measures to counter illegal goods, services, or content online** | Trusted flaggers | | | √ | √ |
| | Measures against abusive notices and counter-notices | | | √ | √ |
| | Vetting credentials of third-party suppliers ("KYBC") | | | √ | √ |
| | Reporting criminal offences | | | √ | √ |
| | Risk management obligations and compliance officer | | | √ | √ |
| | Codes of conduct | | | | √ |
| **Access for researchers to key data** | Data sharing with authorities and researchers | | | | √ |

**Figure 2:** New obligations for gatekeepers in the DSA

### 3.2 United Kingdom – Online Safety Act (OSA)

The OSA focuses on illegal content, child safety, and platform governance. Ofcom is phasing in codes and guidance, including for dis/misinformation via service terms and an Advisory Committee on Disinformation and Misinformation (first meeting planned April 2025). Recent court activity confirms the OSA's reach while highlighting classification and proportionality questions for "Category 1" services.

### 3.3 India– IT Rules 2021/2023 (Fact-Check Unit Litigation)

Amendments proposed a government-run Fact-Check Unit (FCU) to flag online content about "any business of the Central Government" as fake/false/misleading, requiring platform compliance. The Supreme Court stayed operationalization of the FCU pending constitutional review, citing serious free-speech concerns.

### 3.4 Singapore – POFMA (2019– )

The Protection from Online Falsehoods and Manipulation Act empowers authorities to issue Correction Directions (often preferred over removals) and, in serious cases, Stop-Communication/Disabling Directions when a false statement of fact is made and action is in the public interest. Critics argue POFMA grants broad discretion and chills speech; government officials defend it as one tool within a wider resilience strategy.

### 3.5 Germany – NETZDG

Germany's Network Enforcement Act requires large platforms to remove "clearly illegal" user content quickly (24 hours/7 days), imposes reporting duties, and enables significant fines. Amendments refined reporting and user complaint processes. NetzDG has been criticized for incentivizing over-blocking but praised for improving transparency and complaints handling.

### 3.6 United States– Section 230 with State-Level Deepfake Rules

The U.S. maintains platform immunity for third-party content under 47 U.S.C. § 230, leaving most disinformation speech lawful under the First Amendment. Debate continues about its scope and reform; meanwhile, states are acting on AI-generated election deepfakes (e.g., 14 states passed rules in 1H-2024; additional states have criminalized deceptive deepfakes).

### 3.7 Brazil – PL 2630 ("FAKE NEWS BILL")

Brazil's comprehensive bill on platform responsibilities, transparency, and content moderation passed the Senate but remains pending in the Chamber of Deputies, amid strong public debate and pushback from platforms and civil society.

## 4. Enforcement and Early Outcomes

- EU DSA: Movement from soft codes (2018–22) to hard obligations; the Commission has begun formal actions and potential penalties for risk management failures. Researcher access and audits are becoming pivotal evidence channels.
- UK OSA: Ofcom is publishing codes in phases through 2025; mis/disinformation is addressed via illegal-content duties, terms-of-service enforcement, and transparency, not via a freestanding "falsehood" offense. Recent litigation (e.g., Wikimedia case) signals ongoing boundaries-testing.
- India: FCU rules are stayed, so platform duties rest on existing IT Rules without the FCU's special authority.
- Singapore: POFMA is actively used (140+ correction directions by mid-2024), typically requiring labels and links to government corrections.
- Germany: NetzDG enforcement includes fines and standardized reporting; criticisms persist regarding due process and over-removal risks.
- U.S.: Section 230 remains intact; regulatory energy has shifted to state deepfake laws for elections and other harms.

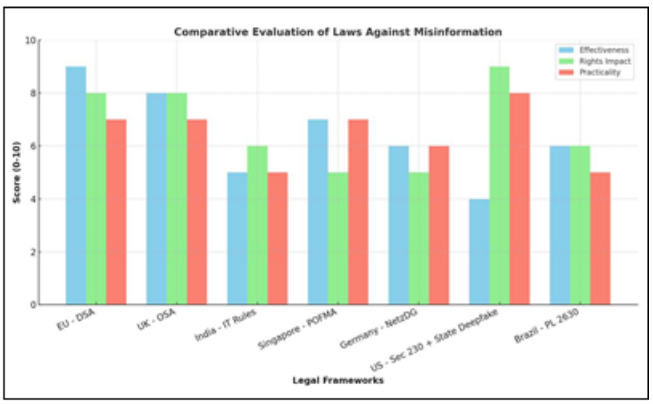


**Figure 3:** Comparative Evaluation of Laws Against Misinformation

## 5. Strengths and Critiques of Current Approaches

**Strengths**

- Systemic risk management (EU/UK): focuses on process, transparency, and mitigation rather than state truth-arbitration.
- Targeted, proportional tools (e.g., POFMA corrections; state deepfake bans): allow context-specific remedies where harms are acute (elections, national security).
- Researcher access & audits (DSA): can improve evidence-based policy and accountability.

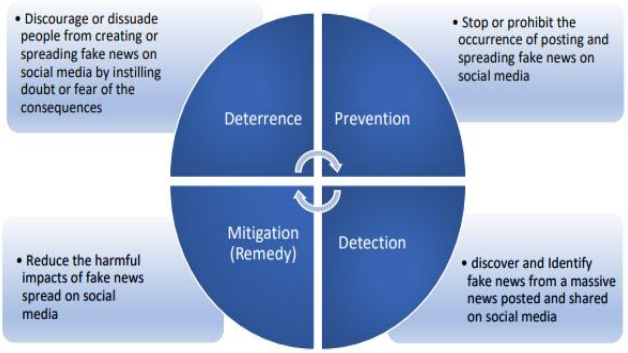


**Figure 4:** A Framework to Combat Fake News on Social Media (Stages and Definitions)

**Critiques**

- Over-delegation to platforms may create incentives to over-remove lawful speech (NetzDG/OSA risk).
- Government discretion risks chilling effects (POFMA; India FCU proposal).
- Fragmentation complicates compliance (U.S. state deepfake patchwork; Brazil's pending bill).
- Due process and transparency gaps remain where notices, appeals, and datasets are not robustly implemented.

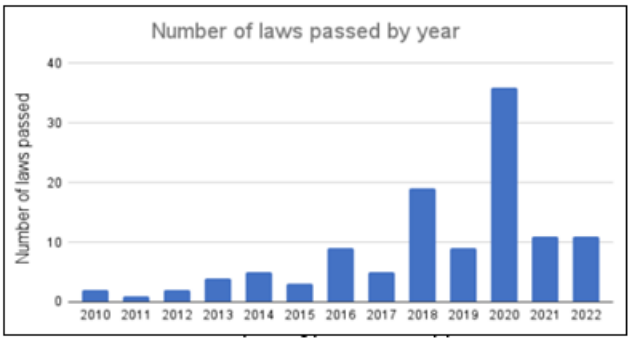


**Figure 5:** Number of laws passed by year

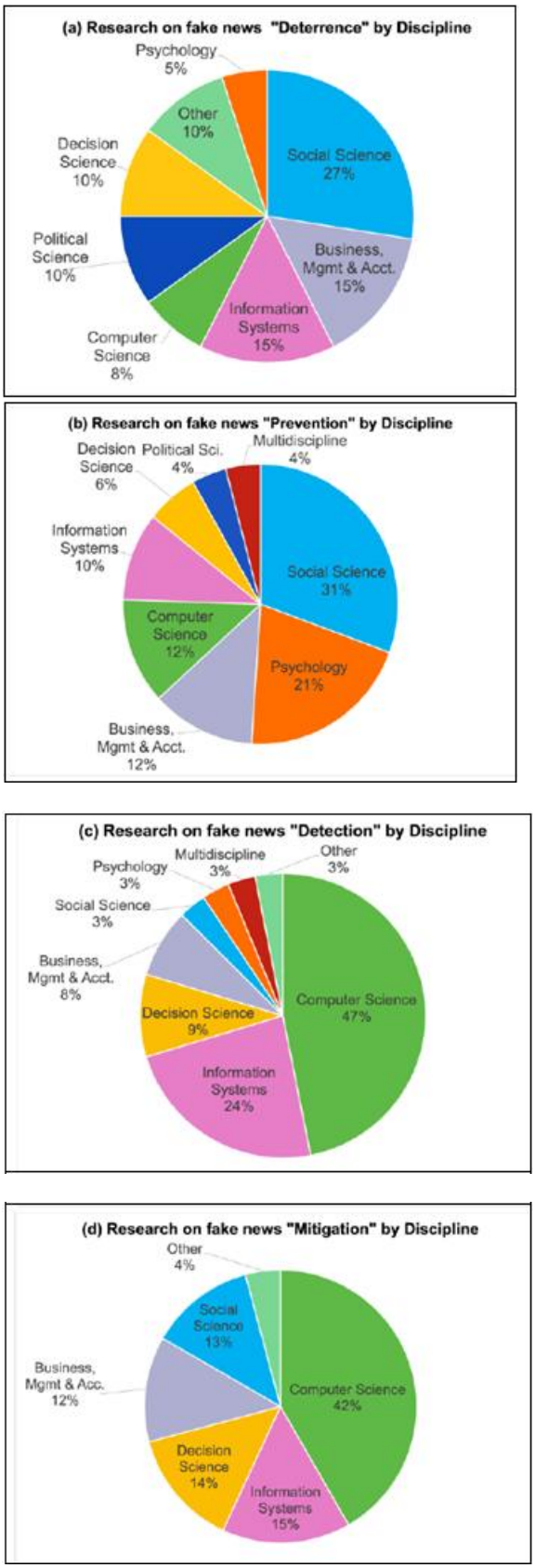


**Figure 6:** Distribution of the Reviewed Articles on Fake News Combat Stages across Disciplines

## 6. Methodologies Used in the Literature

**Recent scholarship blends:**

- Doctrinal analysis of speech protections and intermediary liability;
- Platform governance and risk-based regulation theory;
- Computational social science for measurement of spread and impact;
- Audit studies leveraging DSA researcher-access windows;
- Comparative public law to track convergence and divergence across regimes. See, e.g., recent analyses of disinformation under the DSA.

## 7. Proposed Framework: A Layered, Rights-Preserving Model

**Layer 1- Baseline Duties for All Intermediaries**

- Clear, accessible terms of service; user-friendly notice-and-appeal; periodic transparency reports.
- Basic risk assessment scaled by size and functionality; participation in standardized data-sharing schemas for independent research (privacy-preserving).

**Layer 2 — Elevated Duties for Large/High-Risk Services**

- Systemic risk assessments (elections, public health, information manipulation).
- Independent audits; red-teaming for manipulation vectors; crisis protocols (e.g., violent unrest, pandemics).
- Researcher access with robust safeguards and standardized APIs.

**Layer 3- Targeted Public-Interest Tools**

- Time-bounded correction or labeling for demonstrably false statements of fact in high-risk domains (elections, health), with public-interest tests and independent oversight—a narrower variant of POFMA-style tools. OBJ
- Election deepfake rules focused on synthetic impersonation and material deception near voting periods, with expedited counter-speech access, rapid appeals, and penalties for willful fabrication—aligning with U.S. state trends while preserving core First Amendment protections.

**Cross-cutting Safeguards**

**Strict necessity & proportionality standards;**

- Independent review/appeal (judicial or quasi-judicial) for government orders;
- Whistleblower protections and researcher safe harbors;
- Public logs of significant moderation actions/orders;
- Algorithmic transparency focused on explainability of ranking/recommendation and ad libraries.

## 8. Comparative Evaluation

- Effectiveness: Risk-based regimes (DSA/OSA) are promising where regulators can conduct investigations and require audits. Early indications suggest increasing pressure on large platforms to internalize disinformation externalities.
- Rights impact: Direct takedown powers (NetzDG/POFMA) are fast but risk over-reach without robust appeals and transparency. Courts in India have

already signaled constitutional red lines for broad government fact-checking mandates.

- Practicality: The U.S. model's strong free-speech baseline and Section 230 immunity leave most disinformation to platform policy + civil society countermeasures, with targeted state deepfake rules filling a growing niche. Patchwork risks persist without federal harmonization.

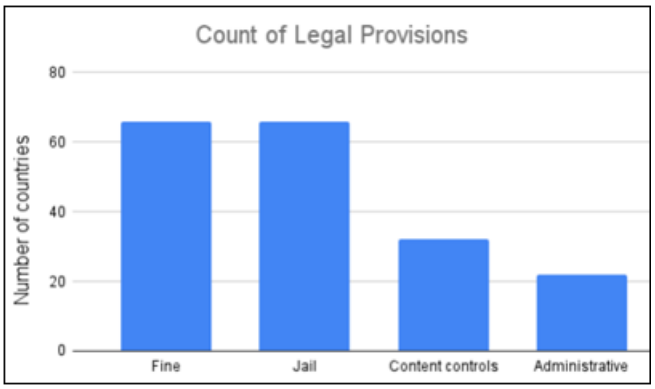


**Figure 5:** Count of Legal Provisions

## 9. Open Research and Policy Gaps

- Measurement of harm and intervention efficacy (labels vs. removals vs. friction).
- Cross-platform manipulation and encrypted messaging dynamics.
- Researcher data access—operationalizing DSA-style access globally without privacy leakage.
- Appeals and remedy design that are fast, fair, and scalable.
- Generative AI: watermarking, provenance, and authentication standards; legal alignment across borders for election periods.

## 10. Conclusion

Around the world, lawmakers are moving from blunt, speech-policing instruments to process-heavy, transparency-first approaches that target systemic risks and empower oversight. The most sustainable path balances platform accountability with fundamental rights, leans on independent audits and researcher access, and uses narrowly tailored, time-bounded tools (especially for elections and synthetic media). Given rapid shifts in platform design and AI capabilities, adaptable, evidence-based regulation with strong due-process guardrails remains essential.

Our findings suggest that most of the fake news research have focused on detection methods and was mostly published in computer science outlets.

## References

[1] Bradshaw, S., & Howard, P. N. (2019). The global disinformation order: 2019 global inventory of organised social media manipulation. Oxford Internet Institute, University of Oxford. https://comprop.oii.ox.ac.uk/research/global-disinformation-order-2019

[2] Gorwa, R., & Garton Ash, T. (2020). Democratic transparency in the platform society. Social Media + Society, 6(2), 1–12. https://doi.org/10.1177/2056305120926482

[3] Heldt, A. P. (2019). Reading between the lines and the numbers: An analysis of the first NetzDG reports. Internet Policy Review, 8(2). https://doi.org/10.14763/2019.2.1413

[4] Tambini, D. (2021). The governance of online disinformation: Theory and practice. Journal of Communication, 71(3), 491–512. https://doi.org/10.1093/joc/jqab004

[5] European Commission. (2024). Digital Services Act – Overview and implementation reports. Publications Office of the European Union. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

[6] UK Parliament. (2023). Online Safety Act 2023: Explanatory notes. The Stationery Office. https://bills.parliament.uk/bills/3137

[7] Supreme Court Observer. (2024). Analysis of IT Rules amendment and Fact Check Unit litigation in India. https://www.scobserver.in

[8] Singapore Law Watch. (2024). Protection from Online Falsehoods and Manipulation Act (POFMA) – Case summaries. https://www.singaporelawwatch.sg

[9] American Bar Association. (2024). Section 230 and content moderation: Current state and reform debates. https://www.americanbar.org

[10] Brennan Center for Justice. (2024). Artificial intelligence and election deepfakes: State legislative approaches. https://www.brennancenter.org

[11] Internet Society. (2023). Analysis of Brazil's PL 2630 fake news bill. https://www.internetsociety.org

[12] Flynn, D. J., Nyhan, B., & Reifler, J. (2017). The nature and origins of misperceptions: Understanding false and unsupported beliefs about politics. Political Psychology, 38, 127–150.

[13] Funke, D., & Flamini, D. (2022, January 21). A guide to anti-misinformation actions around the world. Poynter. https://www.poynter.org/ifcn/anti-misinformation-actions/

[14] Garrett, R. K., & Poulsen, S. (2019). Flagging Facebook falsehoods: Self-identified humor warnings outperform fact checker and peer warnings. Journal of Computer-Mediated Communication, 24(5), 240–258.

[15] Gencheva, P., Nakov, P., Màrquez, L., Barrón-Cedeño, A., & Koychev, I. (2017). A context-aware approach for detecting worth-checking claims in political debates. Proceedings of the International Conference Recent Advances in Natural Language Processing, RANLP 2017, 267–276.

[16] George, J. F., Gupta, M., Giordano, G., Mills, A. M., Tennant, V. M., & Lewis, C. C. (2018). The effects of communication media and culture on deception detection accuracy. MIS Quarterly, 42(2), 551–575.

[17] Gimpel, H., Heger, S., Olenberger, C., & Utz, L. (2021). The effectiveness of social norms in fighting fake news on social media. Journal of Management Information Systems, 38(1), 196–221.

[18] Golbeck, J., Mauriello, M., Auxier, B., Bhanushali, K. H., Bonk, C., Bouzaghrane, M. A., Buntain, C., Chanduka, R., Cheakalos, P., & Everett, J. B. (2018). Fake news vs satire: A dataset and analysis.

Proceedings of the 10th ACM Conference on Web Science, 17–21.

[19] Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. Journal of Management Information Systems, 13(4), 29–47.

[20] Haciyakupoglu, G., Hui, J. Y., Suguna, V. S., Leong, D., & Rahman, M. F. B. A. (2018). Countering fake news: A survey of recent global initiatives