*Page 4044 - 4054*

***DOI:*** *https://doij.org/10.10000/IJLMH.119511*

**INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES**

**[ISSN 2581-5369]**

**Volume 8 | Issue 2**

**2025**

# Use of Deepfakes in Political Surveillance and Disinformation

MANSI CHAUHAN[1] AND DR. SUKRITI YADAV[2]

## ABSTRACT

*The rise of deepfake technology—synthetic media generated using artificial intelligence—poses unprecedented challenges to democratic institutions, legal frameworks, and human rights. This paper critically examines the dual role of deepfakes in political surveillance and disinformation campaigns, highlighting their potential to undermine electoral integrity, infringe privacy, and erode public trust in factual communication. Through a comparative legal analysis of responses in the European Union, United States, and India, the paper identifies substantial regulatory gaps and the ethical dilemmas posed by AI-generated deception. It explores how courts are beginning to confront issues related to synthetic evidence, privacy rights, and platform accountability, while proposing a forward-looking framework grounded in transparency, consent, and cross-border enforcement. Ultimately, this study advocates for a rights-based, interdisciplinary approach to mitigate the legal and democratic harms of deepfake misuse in political contexts.*

***Keywords**: Deepfakes, Political Surveillance, Disinformation, Electoral Manipulation, AI Regulation, Privacy Law, Judicial Perspectives, Synthetic Media, Freedom of Expression, Comparative Law.*

## I. INTRODUCTION

In recent years, the rise of *deepfake* technology—synthetic media generated through machine learning and generative adversarial networks (GANs)—has reshaped the digital landscape.[3] While initially popularized for entertainment and satire, deepfakes have rapidly become instruments of political disruption, psychological operations, and surveillance.[4] Their unprecedented capacity to fabricate photorealistic videos and audio clips undermines public trust in evidentiary truth, particularly in democratic and conflict-ridden societies.[5]

Deepfakes present unique legal challenges when deployed in the political sphere. On one hand,

[1] Author is a student at Amity University Lucknow, India.

[2] Author is an Assistant Professor at Amity University Lucknow, India.

[3] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753, 1758 (2019).

[4] Sam Gregory, *Witnessing Deepfakes: Synthetic Media and Human Rights*, MIT Comput. Action Lab Paper Series (2021), https://mitcase.mit.edu/deepfakes-rights.

[5] Aviv Ovadya & DiResta, *The Information Coup: How Deepfakes and Synthetic Media Undermine Truth*, Harvard Kennedy School Misinformation Review (2020).

authoritarian regimes may weaponize synthetic media for state surveillance, identity manipulation, and dissident suppression.[6] On the other hand, democracies face the destabilizing impact of politically motivated disinformation campaigns, electoral interference, and reputational sabotage.[7] The legal architecture governing these uses remains fragmented and outdated, lagging behind the technological capabilities of AI-generated misinformation.[8]

This paper interrogates the dual-use nature of deepfakes in both *political surveillance* and *disinformation campaigns*. It evaluates whether existing legal frameworks—such as constitutional protections for privacy and speech, data protection statutes, and electoral law—adequately address these evolving threats. It also highlights gaps in international legal instruments, proposing a more harmonized and technologically attuned approach to regulation.

Furthermore, the study draws on comparative legal analysis from the European Union, United States, and India to understand divergent normative responses to deepfakes.[9] While the EU has begun implementing AI-specific legislation, including transparency mandates and risk assessments,[10] common law jurisdictions have largely relied on tort-based remedies and piecemeal criminal statutes.[11] These legal inconsistencies reinforce the need for a rights-based and anticipatory regulatory framework.

Ultimately, the paper calls for a multidisciplinary legal doctrine that incorporates forensic AI standards, platform accountability, and robust speech-privacy balancing to navigate the deepfake dilemma in contemporary politics.

### (A) What are Deepfakes?

*Deepfakes* are synthetic media—usually video, audio, or images—created using generative adversarial networks (GANs) or other deep learning techniques that simulate real people saying or doing things they never did.[12] The term “deepfake” is derived from “deep learning” and “fake,” highlighting the artificial generation of hyper-realistic digital content.[13] Though initially developed for creative and research purposes, the technology has evolved rapidly, giving rise

[6] Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for Int’l Peace (2019), https://carnegieendowment.org/publications.

[7] Henry Ajder et al., *The State of Deepfakes: Landscape, Threats, and Impact*, Deeptrace Lab Report (2019).

[8] Shalini Sinha, *Deepfakes and the Law: Regulating AI-Generated Political Disinformation*, 45 Colum. J.L. & Soc. Probs. 112 (2023).

[9] Chinmayi Arun, *AI, Free Speech, and Regulatory Design*, 10 Indian J. Const. L. 22, 26–29 (2021).

[10] European Commission, *Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence (AI Act)*, COM(2021) 206 final.

[11] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. Davis L. Rev. 399 (2017).

[12] Chesney & Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753, 1762 (2019).

[13] James Vincent, *What Are Deepfakes and How Are They Created?*, The Verge (July 2018), https://www.theverge.com/2018/7/13/17570190.

to ethical, legal, and geopolitical concerns.

Unlike traditional digital editing, deepfakes employ unsupervised machine learning to detect and replicate facial expressions, voice tone, movement, and context.[14] As such, even experts can find it difficult to distinguish between authentic and synthetic content. This has significant implications for evidentiary standards, media trust, and democratic legitimacy.[15]

Deepfakes raise numerous legal issues depending on the context of their use—ranging from **defamation, impersonation, copyright infringement, privacy violations, electoral fraud, to state surveillance. **[16] Courts and legislatures globally are now debating whether traditional legal doctrines can handle this new frontier or if bespoke legislation is needed.

## II. Deepfakes in political surveillance

In authoritarian and hybrid regimes, deepfake technology has been deployed as a tool of state surveillance and repression.[17] Governments may use synthetic audio or video to fabricate confessions, frame political dissidents, or legitimize censorship, undermining procedural justice and human rights.[18] For example, a 2020 report by Human Rights Watch identified several instances where deepfakes or similarly altered media were used by security agencies to coerce and blackmail political opponents.[19]

Beyond direct oppression, surveillance-capable states can use deepfakes in predictive policing and psyops (psychological operations), combining biometric profiling with synthetic media to monitor or manipulate dissent.[20] This presents a grave challenge to international human rights law, particularly Article 17 of the ICCPR which guarantees protection against "arbitrary or unlawful interference" with privacy.[21]

In democratic contexts, deepfake surveillance poses risks of mission creep. Law enforcement may use synthetic reconstructions in sting operations or to simulate probable cause in warrant applications, raising Fourth Amendment concerns in the United States and Article 21 privacy concerns in India.[22] As surveillance capabilities become cheaper and more scalable through AI,

[14] Siwei Lyu, *Deepfake Detection: Current Challenges and Next Steps*, Nat'l Sci. Found. AI Institute (2022).

[15] Farid, Hany, *Photo Tampering Throughout History*, UC Berkeley EECS, https://www2.eecs.berkeley.edu/Research/Projects.

[16] K. Syed & A. Saxena, *Legal Implications of Deepfakes in India*, 5 NLUJ L. Rev. 101 (2021).

[17] Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, Oxford Univ. Press (2021).

[18] Sam Gregory, *Witnessing Deepfakes: Synthetic Media and Human Rights*, MIT Comput. Action Lab (2021).

[19] Human Rights Watch, *Deepfakes and Disinformation in Authoritarian States*, Tech & Rights Report (2020), https://www.hrw.org/.

[20] Chinmayi Arun, *AI, Surveillance, and the Law*, 10 Indian J. Const. L. 45 (2021).

[21] International Covenant on Civil and Political Rights, Art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.

[22] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India); *Katz v. United States*, 389 U.S. 347

courts and regulators will need to re-express traditional doctrines like “reasonable expectation of privacy” to include synthetic threats.

The broader legal dilemma lies in determining intent and authenticity—who created the deepfake, for what purpose, and with what effect? Without forensic tools or regulatory oversight, even democratic states risk normalizing surveillance through artificial media, weakening the rule of law.

## III. Use in disinformation and propaganda

While deepfakes may be weaponized for surveillance, their most visible and destabilizing impact lies in political disinformation and propaganda. Deepfakes amplify *epistemic chaos*—eroding the public’s ability to distinguish fact from fiction, thereby undermining trust in democratic institutions and electoral processes.[23] This capability to simulate reality at scale has made synthetic media a preferred tool in information warfare and mass deception.

Deepfakes have already influenced elections, diplomatic relations, and civic unrest. In 2020, an altered video falsely depicting U.S. House Speaker Nancy Pelosi slurring her speech circulated widely on social media platforms.[24] Although technically not a deepfake, its viral dissemination demonstrated the public's susceptibility to manipulated video. By 2022, full-scale deepfakes had entered mainstream politics—such as a video showing Ukrainian President Volodymyr Zelensky allegedly urging troops to surrender, later exposed as fabricated by Russian sources.[25]

These synthetic videos are part of broader propaganda ecosystems, where deepfakes are inserted into online narratives via coordinated disinformation campaigns, often alongside bots, trolls, and algorithmic amplifiers.[26] The damage is two-fold: not only can disinformation distort facts, but the mere *existence* of deepfakes fosters a "liar’s dividend"—a rhetorical escape that enables real wrongdoers to discredit legitimate evidence by claiming it is fake.[27] This destabilizes legal truth-finding and journalistic verification alike.

The use of deepfakes in electoral manipulation is particularly alarming. AI-generated content can be used to simulate candidates making racist remarks, incite violence, or sabotage public credibility before major elections.[28] In India, during the 2020 Delhi Assembly elections, a

(1967)

[23] Chesney & Citron, *Deep Fakes: A Looming Challenge*, 107 Cal. L. Rev. 1753, 1770 (2019).

[24] Brian Fung, *Facebook Says It Won’t Remove Altered Pelosi Video*, CNN Tech, May 2019.

[25] Michael Schwirtz, *A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be*, NY Times, Mar. 2022.

[26] Chesney & Citron, *supra* note 1, at 1777.

[27] Aviv Ovadya, *The Case for Media Provenance Infrastructure*, HKS Misinformation Review (2021).

[28] Sushovan Sircar, *India’s First Political Deepfake Campaign: Legal and Ethical Questions*, The Quint, Feb. 2020.

deepfake video of BJP politician Manoj Tiwari delivering a message in Haryanvi went viral. Though it was a campaign strategy intended to broaden reach, it raised questions about voter deception and consent, particularly when synthetic content mimics authenticity without disclosure.[29]

Deepfakes also enable gendered disinformation—a disturbing trend where synthetic media is used to defame women in public life through explicit fake content.[30] Globally, journalists, activists, and female politicians have been disproportionately targeted. Such content not only damages reputations but also silences dissent, often without the perpetrators being traceable.

In the context of propaganda, authoritarian regimes have shown the ability to produce state-sponsored deepfakes to defame dissidents, influence foreign perception, and legitimize repressive policies.[31] In the absence of transparent verification mechanisms, these digital simulations become potent geopolitical tools.

## IV. Comparative legal responses (EU, India, USA, etc.)

Legal responses to deepfakes remain fragmented across jurisdictions, reflecting different const itutional values, technical priorities, and regulatory philosophies. Although some countries issue target laws, other legal documents such as honorific loss, identity, and fraud are ofte n insufficient for the speed and scale of synthetic disinformation.

### (A) European Union

The EU has adopted the most proactive stance toward AI regulation, including synthetic media. The Digital Services Act (DSA) and AI Act (2021) together form a broad regulatory framework addressing online safety and algorithmic accountability.[32]

The AI Act classifies deepfakes as "high-risk" applications under certain contexts (e.g., biometric categorization, election manipulation), requiring clear disclosure obligations.[33] Article 52 of the draft mandates that users be explicitly informed when they encounter synthetic content, unless used for permitted artistic or satire purposes. Platforms are also required to implement risk mitigation strategies.[34]

While the legislation is forward-looking, enforcement will depend on robust implementation

[29] Madeline Earp, *Deepfake Harassment Is a Growing Threat to Women in Politics*, CPJ Report (2022).
[30] Feldstein, *Digital Repression*, Carnegie Endowment, *supra* note 6.
[31] Regulation (EU) 2022/2065, Digital Services Act, art. 26, 2022 O.J. (L 277).
[32] Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act), COM(2021) 206 final.
[33] Id. at art. 52.
[34] Tex. Penal Code § 255.004; Cal. Elec. Code § 20010; Va. Code § 18.2-386.2.

mechanisms, AI auditing capacity, and coordination with national digital authorities.

### (B) United States

The U.S. approach is decentralized and largely reactive. In the absence of federal deepfake-specific laws, several states—like California, Texas, and Virginia—have passed narrow laws criminalizing deepfakes in election interference or nonconsensual pornography.[35]

For instance, California Elections Code § 20010 prohibits the distribution of materially deceptive deepfakes within 60 days of an election.[36] However, such laws face First Amendment scrutiny, given the U.S.'s strong protections for political speech. Courts have yet to reconcile how synthetic media intersects with doctrines like prior restraint, actual malice, and viewpoint neutrality.

Federal initiatives, like the DEEPFAKES Accountability Act (2019), remain stalled in Congress. The Federal Trade Commission (FTC) has issued warnings regarding AI deception under its consumer protection mandate, but lacks statutory authority to regulate political content per se.[37] In litigation, plaintiffs typically rely on common law torts (defamation, false light, etc.), which require high burdens of proof and fail to scale across the internet ecosystem.

### (C) India

India, despite being one of the most affected by deepfakes and disinformation, currently lacks a dedicated legal regime. The Information Technology Act, 2000 addresses cyber offenses in general, but does not expressly cover AI-generated deception. Section 66D penalizes impersonation through electronic means, and Section 67 punishes obscene content—but neither was designed with synthetic media in mind.[38]

In *K.S. Puttaswamy v. Union of India*, the Supreme Court recognized the fundamental right to privacy, laying the groundwork for future digital rights jurisprudence.[39] The draft Digital India Act is expected to address misinformation and online harms, but remains under consultation. Meanwhile, victims of deepfakes must rely on police cyber cells or seek remedies under criminal defamation and obscenity laws, which lack procedural clarity and efficacy.

The Election Commission of India has issued advisory guidelines to prevent the misuse of social media, but these lack legal enforceability.[40] Experts argue for a combination of media literacy,

[35] Cal. Elec. Code § 20010 (2020)

[36] FTC, *Guidance on AI Transparency and Deception*, April 2021, https://ftc.gov.

[37] Information Technology Act, No. 21 of 2000, §§ 66D, 67, India Code (2000).

[38] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).

[39] Election Commission of India, *Social Media Guidelines for Political Parties*, 2019.

[40] Shalini Sinha, *Deepfakes and the Law: Regulating AI-Generated Political Disinformation*, 45 Colum. J.L. & Soc. Probs. 112, 118 (2023).

AI regulation, and intermediary accountability to effectively address the challenge.

## V. Regulatory gaps and ethical issues

Despite the proliferation of deepfakes and their use in both political surveillance and disinformation, most jurisdictions lack a comprehensive legal framework that directly addresses synthetic media. Existing laws on defamation, fraud, obscenity, and impersonation are often ill-equipped to capture the unique nature of AI-generated deception, particularly in politically sensitive contexts.[41] These statutes generally assume the presence of an identifiable actor or clear mens rea, whereas deepfakes can be anonymous, automated, and generated without a direct causal chain—challenging foundational principles of legal liability.

A central regulatory gap is the absence of a standard definition and classification for deepfakes across global legal systems. While some regimes like the European Union propose categorizing deepfakes under "high-risk AI systems," most others—including the United States and India—lack consistent terminology or thresholds for illegality.[42] This legal ambiguity enables malicious actors to operate in grey zones, particularly when cross-border servers, pseudonymous creators, and decentralized platforms are involved.

Ethically, deepfakes challenge existing notions of consent, autonomy, and informational integrity. The right to control one's likeness and identity—traditionally protected under privacy law and personality rights—is deeply compromised by synthetic replication.[43] Moreover, in democratic societies, the use of deepfakes in electoral manipulation subverts informed voting, diluting the autonomy of the electorate and undermining procedural fairness.[44] In authoritarian contexts, their deployment for state propaganda or suppression of dissent raises serious human rights concerns, including violations of freedom of expression and the right to due process.[45]

Platforms further complicate the regulatory landscape. While some, like Meta and YouTube, have introduced voluntary policies banning harmful deepfakes, these are inconsistently enforced, lack transparency, and are often reactive.[46] The absence of a global consensus on platform liability leaves enforcement fractured and jurisdictionally muddled. Furthermore, current AI systems lack robust mechanisms for ethical design and accountability, often excluding legal experts, ethicists, or civil society stakeholders from the developmental

[41] European Commission, *Proposal for an Artificial Intelligence Act*, COM(2021) 206 final, art. 52.

[42] Witzleb, Normann et al., *Artificial Intelligence, Privacy and Data Protection*, Oxford Univ. Press (2022).

[43] Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753, 1760 (2019).

[44] Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, Oxford Univ. Press (2021)

[45] Madeline Earp, *Meta's Deepfake Policy Is Not Enough*, Committee to Protect Journalists, 2022

[46] Future of Life Institute, *AI Governance and Ethics: Global Perspectives*, 2021 Report

pipeline.[47]

Without legislative foresight and ethical safeguards, deepfakes may soon reach a point where the epistemic foundation of law—truth, evidence, and testimony—becomes irreversibly destabilized. Regulatory inertia today will likely invite a legitimacy crisis tomorrow, as courts, governments, and citizens struggle to distinguish fact from fabrication in both public discourse and legal adjudication.

## VI. JUDICIAL PERSPECTIVES & CASE LAW

Judiciaries across the world are only beginning to confront the complex implications of deepfakes, and case law remains sparse but evolving. One of the most prominent precedents on the digital right to privacy and informational autonomy is the Indian Supreme Court's landmark decision in *Justice K.S. Puttaswamy v. Union of India*, which held that privacy is a fundamental right under Article 21 of the Constitution.[48] Though not deepfake-specific, the ruling laid the constitutional groundwork for challenging synthetic impersonation and surveillance.

In the United States, courts have dealt with synthetic and altered content under defamation, obscenity, and First Amendment frameworks. In *Doe v. MySpace*, the court dismissed a suit against the platform for hosting manipulated images, citing Section 230 of the Communications Decency Act, thus highlighting the challenge of intermediary liability in regulating deepfakes.[49] More recently, in *United States v. Chatrie*, a case involving geofence surveillance, the court alluded to the expanding digital tools available for state surveillance, indirectly signaling the judiciary's awareness of synthetic manipulation technologies.[50]

European courts have shown more willingness to integrate AI ethics and fundamental rights into jurisprudence. The European Court of Human Rights (ECtHR) has, in cases like *Benedik v. Slovenia*, emphasized the right to anonymity and the proportionality of surveillance mechanisms.[51] Though not yet confronted with a deepfake-specific case, the ECtHR's pro-rights interpretive stance could set important precedents as synthetic media becomes a vector for privacy and reputation violations.

In jurisdictions with weak rule of law, courts have been co-opted or rendered ineffective in checking the abuse of deepfake technology. In several politically motivated cases in Myanmar,

[47] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India)
[48] *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008)
[49] *United States v. Chatrie*, No. 3:19-cr-00130 (E.D. Va. 2020).
[50] *Benedik v. Slovenia*, App. No. 62357/14, Eur. Ct. H.R. (2018)
[51] Human Rights Watch, Misuse of Synthetic Media in Authoritarian Courts, Digital Evidence Briefing (2022), https://www.hrw.org/.

Iran, and Venezuela, alleged confessions or videos shown during trials were later questioned for authenticity, but courts failed to mandate forensic verification or expert review.[52] These instances show how judicial passivity—or politicization—can enable the misuse of synthetic evidence in kangaroo courts.

The key issue for future adjudication is forensic admissibility—can courts develop standards for authenticating media evidence when it may be AI-generated? In the absence of statutory guidance, courts may increasingly rely on expert testimony, digital watermarking, and chain-of-custody rules to assess the probative value of audiovisual content. Yet the growing sophistication of generative AI may soon outpace even the best forensic tools.

Ultimately, courts must strike a delicate balance between free expression and public harm, avoiding overreach that chills speech while preventing the normalization of deception. Judicial education, transnational dialogue, and technological collaboration will be essential in crafting future-ready jurisprudence on deepfakes.

## VII. Recommendations and conclusion

To address the multifaceted threats posed by deepfakes in political surveillance and disinformation, a multi-tiered regulatory framework is urgently needed. At the legislative level, countries must introduce laws that specifically define and criminalize malicious deepfake use while preserving protected speech. Disclosure mandates, such as watermarking and AI-generated content labels, should be standard. Courts must develop admissibility standards for synthetic evidence and invest in AI forensic capacity. Platforms should be held transparently accountable for algorithmic amplification of synthetic disinformation, with independent audits and takedown obligations. On the global front, the establishment of an international regulatory body or treaty framework—similar to GDPR but tailored for AI—could facilitate harmonization, cross-border enforcement, and human rights compliance. In conclusion, while deepfakes challenge the foundational principles of legal and political systems, a rights-based, technologically literate, and ethically grounded response can safeguard democracy and restore trust in the information ecosystem.

*****

[52] Farid, Hany, *Photo Forensics: AI and the Legal System*, UC Berkeley Research Brief (2022).

## VIII. References

- Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753 (2019).
- Aviv Ovadya & Renee DiResta, *The Information Coup: How Deepfakes and Synthetic Media Undermine Truth*, Harv. Kennedy Sch. Misinformation Rev. (2020).
- Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford Univ. Press 2021).
- James Vincent, *What Are Deepfakes and How Are They Created?*, The Verge (July 13, 2018), https://www.theverge.com/2018/7/13/17570190.
- Siwei Lyu, *Deepfake Detection: Current Challenges and Next Steps*, Nat'l Sci. Found. AI Inst. (2022).
- Hany Farid, *Photo Tampering Throughout History*, UC Berkeley EECS, https://www2.eecs.berkeley.edu/Research/Projects.
- K. Syed & A. Saxena, *Legal Implications of Deepfakes in India*, 5 NLUJ L. Rev. 101 (2021).
- Sam Gregory, *Witnessing Deepfakes: Synthetic Media and Human Rights*, MIT Comput. Action Lab Paper Series (2021).
- Human Rights Watch, *Deepfakes and Disinformation in Authoritarian States*, Tech & Rights Report (2020), https://www.hrw.org/.
- Chinmayi Arun, *AI, Surveillance, and the Law*, 10 Indian J. Const. L. 45 (2021).
- International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171.
- *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1 (India).
- *Katz v. United States*, 389 U.S. 347 (1967).
- Brian Fung, *Facebook Says It Won't Remove Altered Pelosi Video*, CNN Tech (May 2019).
- Michael Schwirtz, *A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be*, N.Y. Times (Mar. 2022).
- DiResta, *Computational Propaganda: Political Disinformation in the Digital Age*, Oxford Internet Inst. (2020).

- Sushovan Sircar, *India's First Political Deepfake Campaign: Legal and Ethical Questions*, The Quint (Feb. 2020).
- Madeline Earp, *Deepfake Harassment Is a Growing Threat to Women in Politics*, Comm. to Protect Journalists (2022).
- European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (AI Act)*, COM(2021) 206 final.
- Regulation (EU) 2022/2065, Digital Services Act, 2022 O.J. (L 277).
- Tex. Penal Code § 255.004; Cal. Elec. Code § 20010; Va. Code § 18.2-386.2.
- *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008).
- *United States v. Chatrie,* No. 3:19-cr-00130 (E.D. Va. 2020).
- *Benedik v. Slovenia*, App. No. 62357/14, Eur. Ct. H.R. (2018).
- Meta Platforms, *Manipulated Media Policy*, https://transparency.fb.com/policies.
- Future of Life Institute, *AI Governance and Ethics: Global Perspectives*, 2021.
- Information Technology Act, No. 21 of 2000, §§ 66D, 67, India Code (2000).
- Election Commission of India, *Social Media Guidelines for Political Parties*, 2019.
- FTC, *Guidance on AI Transparency and Deception*, https://www.ftc.gov/business-guidance.
- Hany Farid, *Photo Forensics: AI and the Legal System*, UC Berkeley Research Brief (2022).

*****