INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

AI-DRIVEN CRIMES AND DEEPFAKE TECHNOLOGY: LEGAL CHALLENGES, FORENSIC LIMITATIONS, AND POLICY RESPONSES IN INDIA

AUTHORED BY - GOURIKA AGANPAL
BBA. LLB (Hons)
IILM University Gurugram,

Abstract

The rapid evolution of Artificial Intelligence (AI) has transformed how information is created and shared, but it has also introduced novel avenues for exploitation. Among the most concerning of these is deepfake technology — the use of sophisticated machine learning techniques to produce convincingly fabricated images, videos, or audio recordings. In recent years, deepfakes have been misused for a range of harmful purposes, including online sexual harassment, identity fraud, political misinformation, and financial scams. Indian law currently addresses some of these harms through provisions in the Information Technology Act, 2000, and the Indian Penal Code; however, neither framework directly contemplates the unique nature of AI-generated content. This gap, coupled with limited forensic expertise in detecting synthetic media, makes both investigation and prosecution difficult. This research examines AI-enabled crimes in India with a particular focus on deepfakes, adopting a doctrinal analysis supported by comparative legal perspectives. It evaluates India's current legal mechanisms alongside international initiatives such as the European Union's Digital Services Act and the United States' DEEPFAKES Accountability Act. Special attention is given to evidentiary and procedural hurdles, such as establishing authenticity and maintaining the chain of custody in digital forensics. The paper concludes by proposing targeted reforms, the creation of specialised investigative units, and public education measures to improve detection, prevention, and accountability. The aim is to offer a coherent strategy for protecting individual rights and preserving trust in the digital ecosystem in the face of rapidly advancing AI technologies.

ISSN: 2582-6433

1. Introduction

The proliferation of Artificial Intelligence (AI) technologies has revolutionised communication, information sharing, and content creation. While these developments have yielded considerable benefits for innovation and accessibility, they have also created new avenues for criminal activity in the digital space. One of the most alarming manifestations of AI misuse is deepfake technology — a method of generating synthetic media that is nearly indistinguishable from authentic content. This technology relies primarily on Generative Adversarial Networks (GANs) and other advanced machine learning algorithms to manipulate or fabricate audio-visual material with a high degree of realism.

In recent years, deepfake technology has moved beyond its initial use in entertainment and creative industries to become a potent tool for malicious purposes. Instances of its abuse range from non-consensual sexual imagery and identity theft to the dissemination of political misinformation and the orchestration of complex financial scams. Such acts constitute a serious form of technology-facilitated crime, threatening not only the privacy and dignity of individuals but also the integrity of democratic processes and public trust in information systems.

India's legal framework currently addresses cybercrime through the Information Technology Act, 2000, supplemented by relevant provisions of the Indian Penal Code, 1860, and the Indian Evidence Act, 1872. While these statutes provide mechanisms to address offences such as identity theft, defamation, and the publication of obscene material, they do not expressly recognise deepfake technology or the unique evidentiary challenges it presents. This legislative gap is compounded by the limited capacity of existing forensic infrastructure to detect and authenticate AI-generated media. As a result, law enforcement agencies often face significant obstacles in attributing culpability, preserving digital evidence, and ensuring successful prosecution.

Globally, jurisdictions are beginning to grapple with similar challenges. The European Union's Digital Services Act introduces obligations for digital platforms to monitor and respond to harmful content, including synthetic media. In the United States, legislative proposals such as the DEEPFAKES Accountability Act seek to mandate content labelling and criminalise the malicious creation or distribution of deepfakes. These comparative legal models offer valuable insights for India in crafting a more targeted regulatory response.

ISSN: 2582-6433

This paper adopts a doctrinal and comparative legal methodology to examine the problem of AI-driven crimes, with deepfake technology as the primary focus. It aims to analyse the existing legal framework in India, identify forensic and procedural challenges, and evaluate policy approaches from other jurisdictions. Based on this analysis, the paper proposes a set of legislative amendments, institutional reforms, and public awareness measures to address the multifaceted threats posed by deepfakes. By integrating legal, technical, and policy perspectives, the research seeks to contribute to the development of a coherent strategy for safeguarding individual rights and public confidence in the digital ecosystem.

2. Technology Background

Deepfake technology represents a specialised application of Artificial Intelligence (AI) that synthesises hyper-realistic digital content by manipulating or generating images, videos, and audio recordings. The underlying architecture most commonly associated with deepfakes is the Generative Adversarial Network (GAN), introduced by Ian Goodfellow in 2014. A GAN comprises two neural networks — a generator, which creates synthetic data, and a discriminator, which evaluates its authenticity. Through repeated iterations, the generator progressively improves its output until the discriminator can no longer reliably distinguish between real and fabricated material.

While deepfake creation initially demanded high computational power and technical expertise, the proliferation of user-friendly AI tools and open-source software has democratised access to the technology. Today, applications such as DeepFaceLab, FaceSwap, and commercially available AI video editors allow even non-experts to produce convincing manipulations. These tools can be used to replace faces in videos, synthesise speech in a specific person's voice, or alter lip movements to match alternative dialogue.

The malicious potential of deepfake technology lies in its ability to bypass traditional indicators of digital manipulation. Unlike earlier forms of doctored media, which often exhibited visible artifacts or inconsistencies, modern deepfakes can mimic lighting, facial expressions, and vocal tone with striking precision. As detection methods improve, so too do the algorithms used to evade them, creating a continuous "arms race" between creators of synthetic media and those attempting to identify it.

ISSN: 2582-6433

Globally, the misuse of deepfake technology has expanded into several domains:

1. Non-consensual sexual imagery — The most prevalent form of deepfake abuse, disproportionately targeting women, often for harassment or reputational harm.
2. Political misinformation — Fabricated speeches or statements attributed to public figures to influence elections or incite unrest.
3. Financial fraud — AI-generated voice cloning used to impersonate executives in fraudulent transactions.
4. Cyber extortion — Threats to release manipulated media unless demands are met.

Statistical data underscores the urgency of addressing deepfake misuse. According to a 2023 report by Deeptrace Labs, 96% of detected deepfake videos were pornographic in nature, with the majority targeting women without their consent. Additionally, the World Economic Forum has identified AI-driven misinformation as a top emerging risk to global stability, ranking it alongside cyberattacks and geopolitical conflict.

In India, reliable statistics on deepfake prevalence are scarce, partly due to underreporting and the absence of a formal classification for such offences. However, anecdotal evidence from cybercrime cells indicates a year-on-year increase in reported incidents, with victims ranging from private individuals to political leaders.

Understanding the technological foundations of deepfake creation is essential for crafting effective legal and forensic responses. The complexity of AI-generated content not only challenges existing evidentiary standards but also necessitates the development of specialised detection tools, collaborative international monitoring frameworks, and proactive public education on media literacy.

3. Legal Framework in India

India's legal architecture for addressing cybercrime is primarily governed by the Information Technology Act, 2000 ("IT Act"), supplemented by provisions of the Indian Penal Code, 1860 ("IPC"), and procedural rules under the Indian Evidence Act, 1872. While these statutes collectively provide a framework to tackle a broad range of technology-facilitated offences, none expressly recognise deepfake technology as a distinct category of criminal conduct. This omission poses challenges for classification, investigation, and prosecution.

ISSN: 2582-6433

3.1 Information Technology Act, 2000

The IT Act was enacted to provide legal recognition for electronic transactions and to combat cyber offences. Several sections may be invoked against deepfake-related misconduct:

- Section 66C — Punishment for identity theft: Criminalises fraudulent use of another person's unique identification features, which could apply to unauthorised use of an individual's likeness or voice in deepfake content.
- Section 66D — Cheating by personation through computer resources: Relevant in cases where deepfakes are used for fraud or impersonation.
- Section 67 & 67A — Publishing or transmitting obscene material: Frequently applied in cases of non-consensual sexual deepfakes. Section 67A carries enhanced penalties for sexually explicit content.
- Section 69A — Blocking public access to information: Provides for government-directed removal of harmful deepfake content, though primarily aimed at intermediary compliance.

While these provisions offer some scope, their applicability often depends on proving intent, knowledge, and identity of the perpetrator — a difficult task in deepfake-related cases.

3.2 Indian Penal Code, 1860

The IPC provides overlapping provisions that may be triggered in deepfake scenarios:

- Section 292 — Criminalises the sale or distribution of obscene material.
- Section 354A — Sexual harassment, including creating or sharing sexually explicit deepfakes.
- Section 499 & 500 — Defamation, applicable to reputational harm caused by manipulated media.
- Section 468 & 469 — Forgery and forgery for the purpose of harming reputation, which could extend to synthetic media.

However, the IPC's language was crafted for conventional offences and often struggles to encompass the complexity of AI-generated synthetic content.

3.3 Indian Evidence Act, 1872

Admissibility of deepfake material as evidence hinges on Sections 65A and 65B, which regulate electronic records. Establishing the authenticity of deepfake evidence is fraught with difficulty, as the defence may challenge the integrity of the digital record. Without reliable forensic tools and certified experts, prosecution may fail to meet the evidentiary burden.

ISSN: 2582-6433

3.4 Key Legislative Gaps

1. Absence of explicit recognition of deepfakes as an offence, leading to piecemeal application of existing laws.
2. Limited forensic capacity to detect and authenticate synthetic media.
3. Jurisdictional ambiguity in cross-border cases where content is hosted or created outside India.
4. Lack of intermediary liability clarity for AI-generated content under Section 79 of the IT Act.

The combination of these factors results in inconsistent enforcement and under-prosecution of AI-driven crimes. Addressing these gaps requires both statutory reform and the development of institutional capabilities tailored to emerging technological threats.

4. Comparative Jurisprudence

Deepfake technology has emerged as a global challenge, prompting several jurisdictions to develop targeted legal and regulatory frameworks. While approaches vary, a common thread is the recognition that existing cybercrime and privacy laws are inadequate to address the speed, scale, and sophistication of AI-generated synthetic media.

4.1 European Union – Digital Services Act (DSA)

The European Union's Digital Services Act, which came into effect in 2024, imposes a duty of care on digital service providers to detect, monitor, and remove harmful content, including synthetic and manipulated media.

Key provisions relevant to deepfakes include:

- Mandatory transparency in content moderation algorithms.
- Obligations for large platforms to conduct systemic risk assessments relating to the dissemination of deepfakes.
- Requirements for content labelling to inform users when media has been digitally altered.

The EU also supports research into deepfake detection tools, providing grants for collaborative projects between academia, tech companies, and law enforcement. However, critics argue that the DSA's focus on platforms does not sufficiently criminalise the creators of malicious deepfakes.

ISSN: 2582-6433

4.2 United States – DEEPFAKES Accountability Act

The proposed DEEPFAKES Accountability Act, introduced in the U.S. Congress, aims to criminalise the malicious creation and distribution of deepfakes.

Key features include:

- Labelling requirements for AI-generated media, including embedded digital watermarks.
- Criminal penalties for producing deepfakes with intent to harass, defraud, or influence elections.
- Exemptions for parody, satire, and journalistic work in the public interest.

Although still pending enactment at the federal level, several U.S. states have passed their own legislation — such as Virginia and California — targeting non-consensual sexual deepfakes and election interference. These laws demonstrate a hybrid approach that combines criminal liability with preventive obligations.

4.3 Australia – Online Safety Act, 2021

Australia's Online Safety Act grants the eSafety Commissioner authority to order the removal of image-based abuse, including AI-generated sexual material.

Distinctive elements include:

- A 24-hour takedown requirement for platforms once notified of harmful deepfakes.
- Powers to impose substantial financial penalties on non-compliant service providers.
- Educational initiatives aimed at promoting digital literacy and safe online practices.

Australia's model emphasises victim support, providing pathways for individuals to report abuse and access counselling services.

4.4 Lessons for India

From these comparative models, several lessons emerge:

1. Explicit statutory recognition of deepfakes as a criminal offence is essential.
2. Platform accountability must be strengthened, with clear takedown timelines.
3. Content labelling and watermarking can enhance detection and deterrence.
4. Victim-centric remedies, including counselling and swift removal of harmful media, should be embedded into law.
5. Cross-sector collaboration — linking government, tech industry, and academia — is critical to developing sustainable detection and prevention mechanisms.

By drawing from these frameworks, India can craft a holistic and adaptive approach to

ISSN: 2582-6433

regulating AI-driven crimes, balancing innovation with the protection of individual rights and societal trust.

5. Forensic Challenges

The prosecution of deepfake-related crimes depends not only on a robust legal framework but also on the ability to detect, authenticate, and preserve AI-generated evidence in a manner that satisfies judicial scrutiny. In India, the forensic response to such offences is hindered by technological limitations, procedural gaps, and a shortage of trained specialists.

5.1 Detection of Synthetic Media

Deepfake detection tools operate by identifying anomalies in facial expressions, lighting, pixelation, or audio patterns that are inconsistent with natural human behaviour. Advanced detection systems use AI-driven algorithms trained on large datasets to distinguish between authentic and manipulated media. However, deepfake creation tools are evolving rapidly, often outpacing the development of detection software.

- Problem of the "arms race": As detection algorithms improve, so do the methods used to evade them, making permanent solutions elusive.
- Accessibility gap: Many high-quality detection tools are proprietary and unavailable to local law enforcement agencies in India.

5.2 Authentication and Attribution

Proving that a particular individual created or distributed a deepfake is a significant forensic challenge. The anonymity offered by Virtual Private Networks (VPNs), encryption, and the use of darknet hosting often obscures the digital trail.

- Attribution hurdles: Even if the content can be traced to a device, proving the intent or involvement of the accused requires corroborative evidence.
- Spoofing risk: An adversary may intentionally plant false trails to mislead investigators.

5.3 Chain of Custody

Under Sections 65A and 65B of the Indian Evidence Act, 1872, the admissibility of electronic evidence hinges on proving that the digital record is authentic and unaltered. In deepfake cases, maintaining an unbroken chain of custody is especially difficult because:

- Digital files are easily duplicated or tampered with.

ISSN: 2582-6433

- Cloud-hosted content may be stored on servers outside Indian jurisdiction, complicating access.

Metadata, essential for verification, can be erased or manipulated.

5.4 Forensic Infrastructure in India

While the Central Forensic Science Laboratory (CFSL) and State Forensic Science Laboratories (SFSLs) have capabilities for image and video analysis, they lack specialised AI-based forensic tools. Delays in case processing due to backlog further erode the timeliness of investigation, allowing harmful content to remain online.

5.5 International Cooperation

Given the cross-border nature of deepfake crimes, effective investigation often requires mutual legal assistance treaties (MLATs) or cooperation under frameworks like the Budapest Convention on Cybercrime. India is not yet a signatory to the Budapest Convention, limiting its ability to secure timely evidence from foreign entities.

6. Policy & Reform Proposals

Addressing the threat posed by deepfake technology in India requires a combination of legislative clarity, institutional strengthening, and public awareness. The following recommendations aim to create a framework that is preventive, punitive, and protective.

6.1 Legislative Amendments

1. Explicit Criminalisation of Deepfakes
    - Introduce a dedicated provision in the Information Technology Act, 2000 to define and criminalise deepfake creation, distribution, and possession with malicious intent.
    - Provide graded penalties depending on the nature of harm — from reputational damage to financial loss or sexual exploitation.
2. Mandatory Labelling of AI-Generated Content
    - Require digital platforms and content creators to embed tamper-proof watermarks or metadata in AI-generated media.
    - Impose penalties on platforms that fail to implement adequate detection and labelling systems.

ISSN: 2582-6433

3. Strengthening Intermediary Liability
    - Amend Section 79 of the IT Act to include a strict takedown timeline (e.g., 24 hours) for harmful deepfake content once notified.
    - Mandate proactive monitoring for high-risk content categories, such as election-related media or non-consensual sexual material.
4. Admissibility Standards for Synthetic Media
    - Amend the Indian Evidence Act, 1872 to include specific provisions for authenticating AI-generated media, supported by certified forensic analysis.

6.2 Institutional and Forensic Reforms

1. Specialised AI Crime Units
    - Establish dedicated cybercrime units at both state and central levels equipped with AI-based forensic tools and trained personnel.
2. National Deepfake Detection Lab
    - Develop a government-supported central facility for researching and deploying cutting-edge detection methods, in collaboration with universities and tech companies.
3. Capacity Building for Law Enforcement
    - Introduce mandatory training modules on AI and synthetic media investigation for police, prosecutors, and forensic experts.
4. Cross-Border Collaboration
    - Consider joining the Budapest Convention on Cybercrime or entering bilateral treaties for faster evidence sharing.

6.3 Public Awareness and Education

1. Digital Literacy Campaigns
    - Launch nationwide programmes to educate citizens on identifying deepfakes, understanding their risks, and reporting suspicious content.
2. Victim Support Framework
    - Create a government-backed support system offering legal aid, counselling, and rapid takedown assistance to victims of deepfake abuse.
3. Industry Partnerships
    - Encourage tech companies and social media platforms to co-fund awareness initiatives and provide user-friendly deepfake detection tools.

ISSN: 2582-6433

6.4 Balancing Regulation with Rights

While stronger regulation is necessary, safeguards must be in place to prevent overreach and protect freedom of expression under Article 19(1)(a) of the Indian Constitution. Any law should be narrowly tailored to address malicious conduct without stifling legitimate uses of AI in art, satire, or education. These proposals, taken together, offer a roadmap for transforming India's response to deepfake crimes from a reactive to a proactive stance — one that combines legal deterrence, technological preparedness, and citizen empowerment.

7. Conclusion & Recommendations

The advent of deepfake technology epitomises the double-edged nature of Artificial Intelligence a tool with immense creative potential that, when misused, can inflict significant harm on individuals, institutions, and democratic processes. In India, the absence of explicit statutory recognition for deepfake-related offences, coupled with limited forensic capacity, has created a regulatory and enforcement gap. While existing provisions under the Information Technology Act, 2000, and the Indian Penal Code, 1860, offer some scope for prosecution, they fall short of addressing the complexity, speed, and cross-border nature of AI-driven crimes.

Comparative models from the European Union, the United States, and Australia demonstrate that effective governance of deepfake misuse requires a multi-pronged approach: clear legal definitions, platform accountability, rapid content removal, robust forensic capabilities, and victim-centred remedies. India's current framework can be strengthened by learning from these jurisdictions while tailoring solutions to its socio-legal context.

The key recommendations emerging from this study are:

1. Legislative reform to criminalise malicious deepfakes explicitly, coupled with mandatory labelling of AI-generated content.
2. Institutional strengthening through specialised AI crime units, enhanced forensic infrastructure, and cross-border cooperation mechanisms.
3. Public engagement via digital literacy campaigns, victim support systems, and industry partnerships to counteract misuse at the grassroots level.
4. Balanced regulation that safeguards fundamental rights, ensuring that lawful uses of AI — in art, satire, and innovation — are not unduly curtailed.

ISSN: 2582-6433

Ultimately, addressing deepfake-related offences demands a coordinated, interdisciplinary strategy that blends law, technology, and public policy. By acting decisively now, India can not only mitigate the risks posed by deepfakes but also establish itself as a leader in responsible AI governance. This is not merely a legal imperative but a societal one, ensuring that the digital ecosystem remains a space of trust, safety, and innovation for all.

References

1. Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
2. Indian Penal Code, No. 45 of 1860, INDIA CODE (1860).
3. Indian Evidence Act, No. 1 of 1872, INDIA CODE (1872).
4. Digital Services Act, Regulation (EU) 2022/2065, 2022 O.J. (L 277) 1.
5. DEEPFAKES Accountability Act, H.R. 3230, 116th Cong. (2019).
6. Online Safety Act 2021 (Austl.).
7. Ian Good fellow et al., Generative Adversarial Nets, in Advances in Neural Information Processing Systems (2014).
8. Deeptrace Labs, The State of Deepfakes (2023), https://sensity.ai/reports/.
9. World Economic Forum, Global Risks Report 2023, https://www.weforum.org/reports/global-risks-report-2023/.
10. NITI Aayog, Responsible AI for All: Strategy for India (2021), https://www.niti.gov.in/.
11. Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185.
12. Virginia State Law, Act to Amend the Code of Virginia to Include Deepfake Provisions, ch. 692, 2019 Va. Acts.
13. California Assembly Bill No. 602, Chapter 686, 2019 Cal. Stat.
14. United Nations, Guidance Note on Addressing Technology-Facilitated Gender-Based Violence (2022).