INDIAN GOVERNANCE AND POLICY PROJECT

IGAP PRIMER

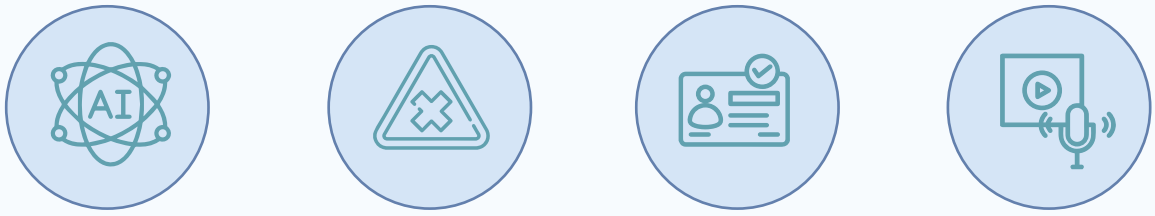
Global Legal Responses to Deepfakes: A Regulatory Primer

Author: **Jhanvi Anam**
Editor: **Shachi Solanki**

Table of Contents

Introduction

Deepfake, a term derived from "deep learning" and "fake", refers to the use of artificial intelligence to generate or manipulate images, audio, or video in ways that convincingly resemble authentic content.[1] A key characteristic of deepfakes is their intent to deceive, manipulating audiences into accepting fabricated events as factual occurrences.[2]



The risks posed by deepfakes are significant and multifaceted, impacting individuals, societies, and nation states by enabling disinformation, reputational harm, privacy violations, and threats to democratic institutions. The weaponisation of deepfakes amplifies systemic risks by eroding public trust, fostering social discord, and threatening national security.

Deepfakes facilitate identity-based crimes and sophisticated fraud schemes that defraud victims of substantial sums. Notably, their most pervasive harm is image-based sexual abuse, with over 96% of publicly available deepfake content comprising pornographic videos and 99% of those depicting women and girls.[3] These non-consensual intimate images are engineered to humiliate, extort, and harass victims.

They can inflict severe reputational damage, portraying individuals in compromising or false scenarios that tarnish careers, relationships, and public standing. Privacy violations occur when personal images, voices, or likenesses are manipulated without consent, stripping individuals of control over their digital identities.

A particularly concerning dimension of deepfakes is their expanding role in electoral processes. Deepfakes have increasingly been used to produce fabricated campaign materials that distort public perception and reshape the political landscape. These synthetic media campaigns threaten the integrity of democratic processes by undermining voters' ability to distinguish authentic political discourse from algorithmically generated propaganda.

Moreover, deepfake technology plays a growing role in information warfare. Nation-states employ deepfakes to fabricate statements attributed to world leaders, create false military communications, and disseminate disinformation aimed at destabilizing adversaries and influencing public opinion.

This multidimensional threat landscape has triggered global regulatory responses, with countries worldwide crafting laws to preserve democratic integrity, protect individual dignity, and maintain societal trust in digital communications. This primer captures the evolving deepfake governance frameworks across the globe. It provides a comparative overview of how different jurisdictions are regulating the harms from deepfake technology, with attention to definitions, platform obligations, criminal liabilities, and civil penalties.

Overview of Global Regulatory Approaches to Deepfake Governance

01. Australia

Legislative Framework

Online Safety Act, 2021[4] - Defines "intimate image" to include material that "depicts or appears to depict" private parts or private activities in circumstances where privacy would be expected. **It is immaterial whether the material has been altered, thereby including deepfakes depicting intimate imagery within the scope of prohibited illegal content.**[5]

Criminal Code Amendment (Deepfake Sexual Material) Act, 2024[6] - Creates specific criminal offences for transmitting sexually explicit material via carriage service without consent. The provisions specifically cover material that has been created, or altered in any way using technology, including AI.[7]

Platform Obligations

Online Safety (Basic Online Safety Expectations) Determination, 2022[8] requires providers of social media, messaging, gaming, and app services to:

- Take reasonable steps to reduce distribution of non-consensual intimate images
- Maintain effective mechanisms for reporting and lodging complaints

Compliance with the expectations is not mandatory. However, the eSafety Commissioner can issue mandatory reporting notices and determinations requiring providers to demonstrate compliance with safety expectations.[9]

Civil Liability

The eSafety Commissioner is authorized to take enforcement action against:

- **End users:** Removal notices and remedial directions for sharing intimate images without consent
- **Service providers:** Removal notices and remedial directions
- **Search engines:** Link deletion and blocking notices
- **App stores:** App removal notices

Criminal Liability

Primary Offence (Section 474.17A):

- Using carriage service to transmit sexual material of adults (18+) without consent
- Covers material that is unaltered, created, or altered using technology (including AI generated deepfakes)
- **Penalty:** Maximum 6 years imprisonment

Aggravated Offences (Section 474.17AA):

- **Repeat offenders:** After 3+ civil penalty orders under Online Safety Act 2021
- **Creator:** Person responsible for creating or altering the sexual material
- **Penalty:** Maximum 7 years imprisonment for both aggravated offences

02. Canada

Legislative Framework

The Criminal Code –[10]
Child pornography includes any photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means, showing children in explicit activity.[11]
The Canadian Supreme Court in R v. Sharpe (2001) read this definition to include deepfakes.

Online Harms Act (Bill C-63) –[12]
This Bill intended to target intimate content communicated without consent, including deepfake sexual images. However, it terminated following prorogation of Parliament in January 2025.

Platform Obligations

Canada does not have any specific platform obligations for deepfakes or intimate images under federal law. British Columbia and Quebec have enacted laws to enforce platform compliance with court ordered takedown requests.

Criminal Liability

Making child pornography and distribution, etc. of child pornography.[13]	**Indictable offence:** Imprisonment for a minimum of 1 year and up to14 years.
Possession of child pornography and accessing child pornography[14]	**Indictable offence:** Imprisonment from 1 year up to 10 years or **Summary conviction:** Imprisonment from 6 months up to 2 years less a day.

03. China

Legislative Framework

→ **Provisions on the Administration of Deep Synthesis Internet Information Services (the Provisions)**[15] – Defines deep synthesis technology as the use of deep learning, virtual reality, and other generative algorithms to create text, images, audio, video, virtual scenes, or similar content.[16]

→ **The Measures for Labeling of AI-Generated Synthetic Content, 2025 (the Measures)**[17] – Defines AI generated synthetic content as text, images, audio, video, virtual scenes, or other information that is generated or synthesized using AI technology.[18]

→ **Interim Measures for the Management of Generative Artificial Intelligence Services (GenAI Measures)**[19] – The GenAI Measures apply to anyone who develops and uses generative AI products to provide service to the public in China. It defines generative AI technology as models and relevant technologies that have the ability to generate content such as texts, images, audio, or video.[20]

Platform Obligations

Deep synthesis service providers are required to have the following measures:

- **Misinformation response:** Quickly correct false information, maintain records, and report to authorities when deep synthesis services spread false information.[21]
- **Security assessments:** Conduct safety assessments independently or through professional bodies.[22]
- **Content labelling:** Add conspicuous notification labels in appropriate places for public facing content.[23]
- **Metadata embedding:** Service providers shall add implicit labels to the metadata of generated synthetic content files.[24]
- **Pre-listing verification:** Internet application platforms must verify labeling materials for synthetic content before allowing an app to be listed.[25]

Civil Liability

Providers of generative AI services:
Subject to enforcement and penalties under existing laws, including the Cybersecurity Law, Data Security Law, Personal Information Protection Law, and the Law on Scientific and Technological Progress. Where no penalties are specified, regulators may issue warnings, public criticism, or rectification orders within a set timeframe.[26]

Users:

- The revised Law on the Protection of Women's Rights and Interests prohibits sexual harassment through verbal, written, image-based, physical, or other unwanted behaviour.
- The Civil Code provides protection of personal rights including privacy, portrait, and reputation with civil damages.[27]

Criminal Liability

- The Cybersecurity Law prohibits the use of networks to endanger national security, disrupt social order, or infringe lawful rights.[28]
- Creation and dissemination of false information to disturb public order or damage reputation is penalised with imprisonment up to 3 years or fine.
- Imposes criminal penalties for using deepfakes to impersonate others for fraud.

04. European Union

Legislative Framework

The EU Artificial Intelligence Act: Deepfakes are defined as AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.[29] The Act establishes an overarching definition and obligations, transposed by individual Member States into national law.

Platform Obligations

EU AI Act

Transparency obligation on deployers: Publishing AI-generated or manipulated image, audio or video content that constitutes a deepfake, must be clearly disclosed as artificial.

Exception: The obligation does not apply when use is:

- Authorised by law to detect, prevent, investigate or prosecute criminal offences, or
- For evidently artistic, creative, satirical or fictional works, with disclosure in an appropriate manner that does not hamper enjoyment of the work.[30]

EU Digital Services Act (DSA)

Notice and action framework: providers must offer accessible systems for users to flag **illegal content**[31]

Content removal: providers having actual knowledge, must expeditiously remove or disable access to the illegal content, or risk losing its liability exemptions.

Civil Liability

Member States must set penalties that are effective, proportionate, and dissuasive.[32]

05. France

Legislative Framework

Law to Secure and Regulate the Digital Space (sécuriser et réguler l'espace numérique (SREN Law)[33] amended[34] the French Criminal Code to criminalise the non-consensual use of algorithmically generated content. This includes **making available to the public or a third party**, by any means, visual or audio content generated by algorithmic processing that represents a person's image or words without their consent.

Platform Obligations

Platforms operating in France must still comply with EU law, including EU AI Act's disclosure duty for deployers and the EU Digital Services Act (DSA)'s notice and action framework.

Criminal Liability

Article 226-8-1 of the French Criminal Code prohibits the distribution of algorithmically generated visual or audio sexual content that depicts a person's image or voice **without their consent,** even where it is apparent or explicitly disclosed that the material is a deepfake.

Penalties depend upon the mode of dissemination:

- For online public communication services, such as a social network, the penalty is up to 2 years in prison and/or a fine of up to 45,000 Euros.
- Private communications like email or instant messaging are not considered online public communications. Sharing non-consensual content via these private channels is subject to lesser penalties.

06. India

Legislative Framework

- **The Information Technology Act, 2000** penalises the act of cheating by personation using any communication device or computer resource.[35] It further addresses the fraudulent or dishonest use of another person's electronic signature, password, or "unique identification feature"[36] and also penalises, publishing or transmitting obscene material in electronic form.[37]
- Under **the Bhartiya Nyay Sanhita** deepfake misuse may fall under offences such as defamation (damaging a person's reputation), intentional insult intended to provoke a breach of peace, and acts or gestures intended to insult the modesty of a woman.
- **Provisions of the Protection of Children from Sexual Offences Act** apply where a child is targeted for pornographic purposes in simulated sexual acts, with or without consent, and for storage of pornographic material involving a child.[38]

Platform Obligations

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, notified under the Information Technology Act, 2000, require:

- **Due diligence:** platforms must make reasonable efforts to ensure their users do not post or share content that:[39]
  - belongs to someone else without rights,
  - is obscene, pornographic, paedophilic, or invasive of privacy,
  - insults or harasses on gender, religion, caste or other grounds,
  - harms children, infringes intellectual property, or spreads false or misleading information,
  - impersonates others, threatens India's security or public order, or contains viruses or harmful code.
- **Content takedown:** Intermediaries must remove or disable access to unlawful information within 36 hours of receiving an order from a court or a notice from the government or its agency.

Criminal Liability

Information Technology Act, 2000	Identity theft, cheating by personation[40]	Imprisonment for up to three years and fine up to INR 1,00,000.
	Publishing transmitting material containing sexually explicit act (including children)[41]	Imprisonment for up to three years and fine up to INR 10,00,000.
Bhartiya Nyay Sanhita	Defamation[42]	Imprisonment for a term which may extend to two years, or with fine, or with both or with community service.
Protection of Children from Sexual Offences	Using a child for pornographic purposes in simulated sexual acts	Imprisonment for a term not less than five years and fine. In the event of second or subsequent conviction imprisonment not less than seven years and fine.

07. Singapore

Legislative Framework

The Elections (Integrity of Online Advertising) (Amendment) Act, 2024 bans "manipulated online election advertising containing realistic but false representation of candidates."[43] This includes any audio or visual or audiovisual depiction created wholly or partly using digital generation or manipulation.

Platform Obligations

Platforms, including social media services, must comply with removal directions issued by authorities. Providers that fail to comply, without reasonable excuse, are punishable with a penalty up to 10,00,000 SGD.[44]

Criminal Liability

A person commits an offence during the election period in Singapore if they publish online election advertising that:

- Contains an audio, visual, or audiovisual depiction of a candidate saying or doing something, whether during that election period or at another time;
- Depicts the candidate doing something they did not in fact say or do, but in a manner realistic enough that members of the public could reasonably believe it; and
- Has been created wholly or partly using digitally generated or manipulated content.

Any person convicted for the offence may be liable to a fine not exceeding $1,000 SGD or imprisonment for a term not exceeding 12 months.

08. South Korea 

Legislative Framework

- **The Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes** penalizes any person who edits, synthesizes, or processes media against the will of the subject in a form that may cause sexual desire or shame, including deepfake pornography.[45]
- **The Public Official Election Act** prohibits producing, editing, distributing, screening, or posting deepfake videos for election campaigning from 90 days before election until polling day.[46]

Platform Obligations

South Korea's Framework Act on the Development of Artificial Intelligence and Creation of a Trust Foundation (South Korean AI Act) requires AI service providers to clearly notify users when audio, images, or video generated by AI are difficult to distinguish from reality. For artistic or creative works, the notice may be given in a way that does not interfere with viewing or enjoyment.[47]

Criminal Liability

Non-consensual deepfake production and distribution has the following penalties:

Distribution	Punishable by imprisonment for not more than 7 years or a fine not exceeding 50 million won.
Distribution for profit	Punishable by imprisonment of minimum three years.
Possession, purchase, storage, or viewing of such content	Punishable by up to three years' imprisonment or a fine of 30 million won
Habitual offenders	Penalties increased by up to half

09. United Kingdom

Legislative Framework

→ **The Online Safety Act, 2023 (OSA)** establishes broad duties for tech platforms to identify, mitigate and manage online harms.[48]

→ The OSA introduced new criminal offences targeting Non-Consensual Intimate Imagery **(NCII)** by amending the **Sexual Offences Act (SOA), 2003**.[49] It criminalizes the specific acts of creating, requesting, and distributing non-consensual intimate images, now including deepfakes.

Platform Obligations

User-to-user services, such as social media platforms and regulated search services are required to:[50]

- Conduct risk assessments to identify harms from illegal content and content harmful to children.[51]
- Carry out a suitable and sufficient children's access assessment.
- Take steps to prevent or minimise user exposure to such content.[52]
- Implement proportionate measures to mitigate identified risks.

Civil Liability

Non-compliance with safety duties triggers regulatory action, such as fines and service restrictions.

Criminal Liability

There are four offences relating to NCII incorporated within the SOA, as below:

Offences	Penalties
› Sharing intimate images without consent.[53]	◉ Liable on summary conviction with a maximum of six month imprisonment or a fine or both.[54]
› Sharing intimate images without consent with the intention to cause alarm, distress, or humiliation. [55]	◉ Liable on summary conviction, to imprisonment for a term not exceeding 6 - 12 months or a fine (or both)
› Sharing without consent, or without a reasonable belief in consent, for the purpose of sexual gratification.[56]	◉ After conviction in a serious trial, the maximum punishment is 2 years.
› Threatening to share intimate images with the intention, or reckless disregard of the likelihood, that the person targeted or someone connected to them will fear the threat will be carried out.[57]	

10. United States 

Legislative Framework

The Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act)[58] prohibits the non-consensual online publication of intimate visual depictions, whether authentic or computer-generated.[59]

Platform Obligations

Under the TAKE IT DOWN Act platforms must:

- Set up a process allowing an identifiable individual or an authorized representative to notify the platform of an intimate visual depiction published on it that includes their likeness within 1 year of enactment.[60]
- Upon receiving a valid removal request, remove the intimate visual depiction **within 48 hours** and take reasonable steps to locate and remove any identical copies.

Civil Liability

Failure to reasonably comply with the notice-and-takedown obligations is treated as an unfair or deceptive act or practice under the Federal Trade Commission Act.

Criminal Liability

Offences[61]	Penalties
Publishing a digital forgery of an adult without consent, where content was not publicly exposed, not of public concern, and intended to cause (or does cause) harm.	Up to 2 years' imprisonment, fine, or both.
Publishing a digital forgery of a minor with intent to abuse, humiliate, harass, degrade, or for sexual gratification.	Up to 3 years' imprisonment, fine, or both.
Threatening to publish a digital forgery of an adult to intimidate, coerce, extort, or cause distress.	Up to 18 months' imprisonment, fine, or both.
Threatening to publish a digital forgery of a minor to intimidate, coerce, extort, or cause distress.	Up to 30 months' imprisonment, fine, or both.

Proposed Legislative Developments Targeting Deepfake Technology

Proposed Copyright Act Amendment

The Danish Government has proposed amendments to the Copyright Act to regulate realistic, digitally generated imitations of people's likeness and voice. The proposal gives individuals the right to control such imitations, and to seek takedowns, damages, or bring infringement proceedings. These amendments are under public consultation, with the enactment targeted for January 2026.

The amendments set out two key rules:[62]

- Realistic digital imitations of a performing artist's artistic performance cannot be made available to the public without consent.[63]
- Realistic digital imitations of any person's appearance, voice, or movements cannot be publicly shared without consent. This protection applies even if no copyright work or performance is involved.

Platform Obligations

The proposal provides civil, rights-based protection and does not impose labelling or takedown duties. Platforms in Denmark must still comply with the European Union laws, including the EU AI Act's disclosure duty for deployers[64] and the EU Digital Services Act's notice and action framework, which requires user reporting systems and prompt removal of illegal content to maintain liability exemptions.[65]

Civil Liability

- Copyright enforcement: Infringements of the proposed amendments could trigger liability under copyright rules (for e.g. injunctions, damages and compensation).
- Damages and compensation: Affected parties may pursue claims for damages and compensation according to the general principles of Danish law.

Criminal Liability

The proposed amendments do not create direct provisions for compensation or criminal penalties. However, violations of the rules on digital imitations, when committed intentionally or through gross negligence, are subject to penal sanctions.[66] Importantly, this right is based solely on the unauthorised use of a person's likeness, without the need to demonstrate any actual harm, allowing individuals to seek removal on that ground alone.

02. Germany

Proposed amendment to the Criminal Code

The German Bundesrat proposed [67] a new criminal offence through the addition of Section 201b to the German Criminal Code (Violation of personality rights through digital forgery), seeking to address the growing concern that deepfakes can seriously infringe personal rights.

→ It defines violation of personality rights through digital forgery as the creation or distribution of computer-generated or altered recordings that realistically depict a person's appearance, behaviour, or speech without their consent.[68]

→ It will apply equally to content concerning living or deceased persons.

Platform Obligations

Providers must comply with the EU AI Act and the DSA, as noted in the section on European Union.

! The German Ministry of Justice acknowledged[69] the risks posed by deepfakes, while noting that many harmful uses are already covered by existing criminal law, particularly defamation and violation of the highly personal sphere by producing or transmitting images.

Criminal Liability

The German Criminal Code prohibits:

Offences	Penalties
› Spreading false information about another person that could damage their reputation, harm public opinion of them, or endanger their creditworthiness › Unauthorised creation or distribution of recordings that invade privacy.[70]	Imprisonment for a term not exceeding two years or a fine

03. Switzerland

Switzerland has decided against a dedicated deepfake regulation. The House of Representatives of Switzerland rejected a motion to introduce specific deepfake rules; The Swiss Government's position is to rely on existing, tech neutral laws.[71] Existing tools under criminal and civil laws, including those protecting privacy, already cover deepfakes under Swiss Civil Code. Right to one's own image, injunctions and damages[72] and Federal Act on Data Protection (FADP) applies to AI processing and treats biometric data that uniquely identifies a natural person, as sensitive, triggering stricter duties.[73]

Regulatory Mapping across Jurisdictions

The following table provides a comparative overview of how different jurisdictions address deepfakes and related harms through their regulatory frameworks. It categorizes global approaches based on whether countries have enacted specific deepfake laws or provisions, rely on existing laws to address related harms, or are developing targeted legislation.

Express Definitions	Targeted Coverage	Proposed Legislations
China	Australia	Denmark
European Union	Canada	Germany
Singapore	France	
USA	India	
	South Korea	
	UK	

Table: Regulatory coverage of deepfakes by jurisdiction

FOOTNOTES

1 Biranchi Naryan P. Panda and Isha Sharma, Deepfake Technology in India and World: Foreboding and Forbidding. Available at https://www.asianinstituteofresearch.org/lhqrarchives/deepfake-technology-in-india-and-world%3A-foreboding-and-forbidding

2 Ofcom UK, Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes. Available at https://www.ofcom.org.uk/siteassets/resources/documents/consultations/discussion-papers/deepfake-defences/deepfake-defences.pdf?v=370754

3 Home Security Heroes. (2023). 2023 State Of Deepfakes: Realities, Threats, And Impact. Available at https://www.securityhero.io/state-of-deepfakes/

4 Online Safety Act, 2021, Act No. 127, 2024. Available at https://www.legislation.gov.au/C2021A00076/latest/text

5 Section 15 of the Online Safety Act, 2021.

6 Criminal Code Amendment (Deepfake Sexual Material) Act, 2024. Available at https://www.ato.gov.au/law/view/pdf/acts/20240078.pdf

7 Section 474.17A of the Criminal Code Amendment (Deepfake Sexual Material) Act, 2024.

8 Online Safety (Basic Online Safety Expectations) Determination, 2022. Available at https://www.legislation.gov.au/F2022L00062/latest/text

9 Basic Online Safety Expectations: Regulatory Guidance. Available at https://www.esafety.gov.au/sites/default/files/2024-07/Basic-Online-Safety-Expectations-regulatory-guidance-July-2024.pdf

10 The Canadian Criminal Code. Available at https://laws-lois.justice.gc.ca/eng/acts/c-46/page-26.html#h-118363

11 Section 163.1 of the Canadian Criminal Code.

12 The Online Harms Bill. Available at https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c63.html

13 Section 163.1(2) and Section 163.1(3) of the Canadian Criminal Code.

14 Section 163.1(4) and Section 163.1(4.1) of the Canadian Criminal Code.

15 Provisions on the Administration of Deep Synthesis Internet Information Services (the Provisions). Available at https://www.chinalawtranslate.com/en/deep-synthesis/

16 Article 23 of the Provisions.

17 The Measures for Labeling of AI-Generated Synthetic Content, 2025 (the Measures). Available at https://www.chinalawtranslate.com/en/ai-labeling/

18 Article 3 of the Measures.

19 Interim Measures for the Management of Generative Artificial Intelligence Services (GenAI Measures). Available at https://www.chinalawtranslate.com/en/generative-ai-interim/

20 Article 22 of the GenAI Measures.

21 Article 11 of the Provisions.

22 Article 15 of the Provisions.

23 Article 4 of the Measures.

24 Article 16 of the Provisions and Art 5 of the Measures.

25 Article 7 of the Measures

26 Article 21 of the GenAI Measures

27 Article 3, Article 110 and Article 990 of the Civil Code of the People's Republic of China. Available here http://en.npc.gov.cn.cdurl.cn/pdf/civilcodeofthepeoplesrepublicofchina.pdf

28 Article 12 of the Cybersecurity Law Available at https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

29 Article 3(60) of the EU AI Act

30 EU AI Act Article 50(4)

31 Article 16 of the EU DSA. Available at https://www.eu-digital-services-act.com/Digital_Services_Act_Article_16.html

32 EU AI Act Article 99

33 Sécuriser et réguler l'espace numérique,(SREN Law). Available at https://www.senat.fr/leg/pjl23-051.pdf

34 Blog: France prohibits non-consensual deepfakes. Available at https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes?

35 Section 66D of the IT Act

36 Section 66C of the IT Act. Available here https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

37 Section 67, 67A and 67B of the IT Act

38 Section 13 and 14 of the POCSO Act. Available here https://www.indiacode.nic.in/bitstream/123456789/2079/1/AA2012-32.pdf

39 Rule 3 of the IT Rules, 2021

40 Section 66D of the IT Act

41 Section 67A and 67B of the IT Act

42 Section 356 of the BNS

43 Section 61MA of the Elections (Integrity of Online Advertising) (Amendment) Act, 2024. Available at https://www.parliament.gov.sg/docs/default-source/bills-introduced/elections-(integrity-of-online-advertising)-(amendment)-bill-29-2024.pdf

44 Section 61MA (2) of the Elections (Integrity of Online Advertising) (Amendment) Act, 2024.

45 Article 14-2 of the Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes. Available at https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%84%B1%ED%8F%AD%EB%A0%A5%EB%B2%94%EC%A3%84%EC%9D%98%EC%B2%98%EB%B2%8C%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%ED%8A%B9%EB%A1%80%EB%B2%95

46 Article 82-8 (added by amendment) of the Public Official Election Act. Available at https://www.nec.go.kr/site/eng/ex/bbs/View.do?cbIdx=1270&bcIdx=226657

47 Article 31 of the South Korean AI Act https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%9D%B8%EA%B3%B5%EC%A7%80%EB%8A%A5%20%EB%B0%9C%EC%A0%84%EA%B3%BC%20%EC%8B%A0%EB%A2%B0%20%EA%B8%B0%EB%B0%98%20%EC%A1%B0%EC%84%B1%20%EB%93%B1%EC%97%90%20%EA%B4%80%ED%95%9C%20%EA%B8%B0%EB%B3%B8%EB%B2%95/(20676,20250121)

48 The Online Safety Act. Available at https://www.legislation.gov.uk/ukpga/2023/50

49 Section 188 of the OSA

50 These requirements are set out in Section 9 and Section 11 for user-to-user services and Sections 26 and Section 28 for search services.

51 Article 7 of the OSA

52 Article 10 of the OSA

53 Section 66B(1) of the SOA

54 Section 66B(9) of the SOA

55 Section 66B(2) of the SOA

56 Section 66B(3) of the SOA

57 Section 66B(4) of the SOA

58 Take it down Act. Available at https://www.congress.gov/bill/119th-congress/house-bill/633/text

59 Section 146 of the Take it Down Act. Available at <https://www.congress.gov/bill/119th-congress/senate-bill/146>

60 Section 3 of the Take it Down Act

61 Section 3 of the Take it Down Act

62 Blog: Denmark's Deepfake Legislation: Bold Copyright and Digital Identity Protection. Available at https://abounaja.com/blog/denmarks-deepfake-legislation-bold-copyright-and-digital-identity-protection

63 Section 65a of the proposed amendment to the Copyright Act. Available at https://www.kimavocat.com/post/denmark-proposees-ai-deepfake-copyright-law-to-protect-personal-likeness-voice-and-identity

64 Article 50(4) of the EU AI Act. Available at https://artificialintelligenceact.eu/article/50/#:~:text=4.,been%20artificially%20generated%20or%20manipulated.

65 Digital Services Act. Available at https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

66 Section 76 of the Copyright Act. Available at https://www.wipo.int/wipolex/en/legislation/details/1146

67 Blog: Germany's legal debate on criminal liability for misuse of deepfakes: navigating uncharted waters. Available at https://www.lexology.com/library/detail.aspx?g=9b0c1d2d-a39d-4761-923c-3d8eacf9bb7c

68 Digital Policy Alert, Germany: Introduced Bill relating to criminal protection of personality rights against deepfakes. Available at https://digitalpolicyalert.org/event/21354-introduced-bill-relating-to-criminal-protection-of-personal-rights-against-deepfakes

69 Blog: Germany's legal debate on criminal liability for misuse of deepfakes: navigating uncharted waters. Available at https://technologyquotient.freshfields.com/post/102jisu/germanys-legal-debate-on-criminal-liability-for-misuse-of-deepfakes-navigating

70 Section 201a of the German Criminal Code

71 Swissinfo Blog: Switzerland rejects deepfake regulation. Available at https://www.swissinfo.ch/eng/ai-governance/switzerland-rejects-deepfake-regulation/89277391

72 Article 28 of the Swiss Civil Code. Available at https://www.fedlex.admin.ch/eli/cc/24/233_245_233/en

73 Swiss Confederation: Update - Current data protection legislation is directly applicable to AI. Available at https://www.edoeb.admin.ch/en/update-current-legislation-directly-applicable-ai

INDIAN GOVERNANCE AND POLICY PROJECT

The Indian Governance And Policy Project (IGAP) is an emerging think tank focused on driving growth, innovation, and development in India's digital landscape. Specializing in areas like AI, Data Protection, FinTech, and Sustainability, IGAP promotes evidence-based policymaking through interdisciplinary research. By working closely with industry bodies in the digital sector, IGAP provides valuable insights and supports informed decision-making. Core work streams include policy monitoring, knowledge dissemination, capacity development, dialogue and collaboration.

For more details visit: www.igap.in

Contact us: relations@igap.in