

**Bill No. XXX of 2025**

**THE DEEFAKE (REGULATION AND PROTECTION)  
BILL, 2025**

ARRANGEMENT OF CLAUSES

CLAUSES

**CHAPTER I  
PRELIMINARY**

1. Short title, extent and commencement.
2. Definitions.

**CHAPTER II**

DEEFAKE REGULATORY AUTHORITY

3. Establishment of deepfake regulatory authority
4. Composition of authority
5. Qualifications for appointment as Chairman, Vice-Chairman and other Members
6. Terms of office
7. Resignation and removal
8. Salaries and allowances and other terms and conditions of service of Chairman, and other Members
9. Powers and Functions of authority

**CHAPTER III**

CONSENT AND DISCLOSURE FRAMEWORK

10. Mandatory consent for creation and dissemination.
11. Withdrawal of consent
12. Certain legitimate uses
13. Disclosure obligation
14. General obligations pertaining to preservation of consent records

**CHAPTER IV**

PROHIBITION OF MALICIOUS USES

CLAUSES

15. Prohibition of malicious deepfake creation
16. Prohibition of exploiting intimate content

17. Prohibition of deepfake creation to incite violence, hatred or threatens national security
18. Prohibition of activities relating to unlawful gain
19. Prohibition on distribution of deepfake content by intermediaries

## CHAPTER V

### PROTECTION OF WHISTLEBLOWERS AND INFORMANTS

20. Right to anonymity

## CHAPTER VI

### RIGHTS OF VICTIMS AND REMEDIES

21. Right to seek redressal
22. Right to erasure of previously published deepfake contents
23. Remedies against platform negligence
24. Right to appeal

## CHAPTER VII

### EXCEPTIONS AND SAFE HARBOR

25. Acts not to be offenses
26. Protection for acts done in good faith
27. Exemption of intermediaries from liability
28. Defense of due diligence

## CHAPTER VIII

### TECHNOLOGICAL OBLIGATIONS AND INDUSTRY RESPONSIBILITY

29. Obligation to watermark and disclose AI- Generated content
30. Deployment of detection and labelling mechanisms
31. Maintenance of transparency reports
32. Responsibility of AI developers and model providers
33. Industry codes of practice.

## CHAPTER IX

### NATIONAL SECURITY AND FOREIGN INTERFERENCE

34. Prohibition of foreign deepfake interference
35. Power to block and restrict access to harmful content
36. Co-ordination with security and election authorities
37. Liability for cross- border malicious campaigns
38. Enhanced Punishment for Repeat Offences
39. Extraterritorial application

## CHAPTER X

### APPEAL AND ALTERNATE DISPUTE RESOLUTION

40. Appeal to appellate Tribunal
41. Orders passed by tribunal to be executable as decree
42. Alternate dispute resolution
43. Enforcement of awards

## CHAPTER XI

### OFFENCES AND PENALTIES

44. Unauthorized creation of deepfakes
45. Dissemination of deepfakes without consent
46. Obscene and sexually explicit deepfakes
47. Deepfakes involving children
48. Defamation and harassment by deepfakes
49. Fraud, impersonation and financial offences offenses by deepfakes
50. Electoral interference through deepfakes
51. Deepfakes prejudicial to sovereignty and national security
52. Malicious us against celebrities and public figures
53. Corporate liability for deepfake offenses
54. Liability of intermediaries and platforms for non-compliance
55. Enhanced punishment for repeated offenders
56. Extra territorial application of offenses

## CHAPTER XII

### OVERSIGHT AND REPORTING

57. Annual compliance reporting
58. Independent audit of AI systems
59. Establishment of transparency portal
60. Parliamentary oversight and reporting

## CHAPTER XIII

### MISCELLANEOUS

61. Power of central government to issue directions
62. Consistency with other laws
63. Power to make rules retrospectively

**THE DEEPFAKE (REGULATION AND PROTECTION)****BILL, 2025**

A

**BILL**

*To protect individuals, celebrities, companies and institutions from the from the adverse social, economic, psychological and privacy-related impacts of deepfakes; to regulate the creation of deepfake across technological platforms; to establish deepfake regulation authority for oversight and to function as grievance redressal mechanism; to promote ethical and responsible use of Artificial intelligence and related technologies; to protect national security against the threats posed by deepfakes and protect sovereignty and security of the state and to provide remedies to victims of such harmful usage of deepfake technology ; to establish a uniform, national-level legal framework in the public interest; and for matters connected therewith or incidental thereto.*

WHEREAS the deepfake technologies has much risen exponentially, promoting redundant manipulated audio-visual content that obscures reality from fakes;

AND WHEREAS such technologies bring opportunities for technological progress, education and creativity, even as they pose alarming threats in relation to deception, harassment, reputational damage, meddling in affairs of the state, electoral meddling, and privacy invasions;

AND WHEREAS persons, particularly celebrities, public figures, child artist are increasingly exposed to exploitation of the deepfake contents;

AND WHEREAS the spread of false contents produced with ill intent imperils public trust, distorts well-informed decision-making, disseminates false information and erodes democratic discourse;

AND WHEREAS the absence of extensive framework to govern the production and publication of deepfakes has led to rising risk of privacy breach also emanating from cross-border digital platforms that exist outside democratic authority;

AND WHEREAS deepfake platforms tend to utilize automatic systems, prejudiced algorithms and AI mechanisms that produce dangerous content warrants unified regulatory institution;

AND WHEREAS deepfake abuse has escalated crimes including identity theft, defamation, production of sexual material, morphing, financial fraud, misleading political content that threatens personal security and national security;

AND WHEREAS it is desirable in public interest that the Union Government constitute the Deepfake regulation authority and grant a formalized legal framework, harmonizing technological progress with ethics, morality and respect for human dignity, safeguarding the people from harm while allowing legitimate use for the aim of entertainment and education.

BE it enacted by Parliament in the Seventy-sixth Year of the Republic of India as follows: —

## CHAPTER I

## PRELIMINARY

1. (1) This act may be called the Deepfake (regulation and protection) Act, 2025.

Short title, extent and  
commencement

(2) It extends to, —

(i) The whole of India; and

(ii) To any offence committed outside India Affecting any individual, company or institution in India or affecting the sovereignty, security or integrity of India

(3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

## Definitions

2. In this Act, unless the context otherwise requires,

- (a) “Actual knowledge” means awareness of the existence of a malicious deepfake, whether by—
  - (i) receipt of a complaint or notice from the Authority or a court of competent jurisdiction; or
  - (ii) detection by the intermediary, platform, or developer itself;
- (b) “Appellate tribunal” means specialized judicial body designated to hear appeals against the authority’s decision;
- (c) “Artificial intelligence system” means any computational system, algorithm, or model, including machine learning, deep learning, or generative models, capable of creating, manipulating, or detecting deepfakes;
- (d) “Authority” means the regulatory body or designated authority notified by the Central Government under this Act for the purpose of implementation, monitoring, and enforcement;
- (e) “Automated” means any technological process capable of operating automatically in response or the prompt given;
- (f) “Celebrity” means any individual whose name, image, likeness, or persona has commercial value or public recognition, including but not limited to actors, musicians, athletes, artists, social media influencers, and political leaders;
- (g) “Child deepfake” means any deepfake depicting a person who is, or is made to appear as, below the age of eighteen years, in a sexually explicit, abusive, or exploitative manner;
- (h) “Company” shall have the same meaning as assigned under section 2(20) of the Companies Act, 2013, and includes any, body corporate, partnership, limited liability partnership, or association of persons engaged in business;
- (i) “Consent” means free, informed, explicit, and written or digital approval given by the individual so depicted, prior to the creation or dissemination of a deepfake;
- (j) “Deepfake” means any visual, audio, or audiovisual content, generated or manipulated using artificial intelligence, machine learning, or other digital or computational techniques, in such a manner that it falsely depicts, fabricates, or alters the likeness, appearance, voice, or identity of a natural person;
- (k) “Dissemination” includes transmission, forwarding, uploading, reposting, streaming, or

otherwise making a deepfake accessible, directly or indirectly, to one or more persons;

- (l) “Due diligence” means reasonable measures undertaken by an intermediary, company, or platform to prevent the creation, storage, or dissemination of malicious deepfakes, including but not limited to—
  - (i) deployment of detection technologies;
  - (ii) user verification systems; and
  - (iii) maintenance of grievance redressal mechanisms;
- (m) “Impersonation by deepfake” includes the use of synthetic likeness, cloned voice, manipulated face, or any other synthetic representation that would cause a reasonable person to believe the impersonation to be genuine;
- (n) “Intermediary” shall have the same meaning as assigned under section 2(w) of the Information Technology Act, 2000, and includes social media platforms, content-sharing services, search engines, or digital communication platforms;
- (o) “Malicious deepfake” means a deepfake created, used, or disseminated with the intent to deceive, defraud, harass, intimidate, exploit, mislead electors, threaten national security, incite disorder, or otherwise cause wrongful loss or wrongful gain;
- (p) “Manipulated content” means audio, video, text or audio-visual that has been modified, altered, fabricated using digital tools, AI to distort original information, designed to deceive, impersonate or defame.
- (q) “Obscene deepfake” means any deepfake which is lascivious, sexually explicit, depicts nudity, or appeals to the prurient interest in a manner which tends to deprave or corrupt persons likely to view it;
- (r) “Platform” means any intermediary, online service, or application which enables the creation, hosting, transmission, or dissemination of user-generated content, including deepfakes;
- (s) “Publication” means making a deepfake available, whether through electronic means, digital platforms, broadcast, or any medium by which it may be accessed or shared by the public;
- (t) “Public figure” means—
  - (i) any person holding a constitutional, statutory, or elected office; or
  - (ii) any person of political, social, or cultural prominence, including but not limited to members of Parliament, legislators, and judges;
- (u) “Synthetic media” includes deepfakes, unrealistic impersonation, voice cloning and other forms of manipulated content, for the purpose of entertainment, satire or for commercial use with malicious intent;
- (v) “Transparency report” means the periodic report mandated under this Act, containing disclosures regarding complaints, removals, detection, enforcement actions, and cooperation with law enforcement.
- (w) “Watermarking” means the embedding of visible or invisible markers, digital signatures, or other technological identifiers in a deepfake to disclose its synthetic origin.
- (x) “Wrongful gain” and “Wrongful loss” shall have the same meaning as assigned under the BNS, 2023.

21 of 2000

45 of 2023

## CHAPTER II

### DEEPAKE REGULATORY AUTHORITY

3. **Establishment of deepfake regulatory authority.** — (1) With effect from such date as the Central Government may, by notification in the Official Gazette, appoint a body to be called the Deepfake

regulatory Authority for the purpose of this Act.

- (2) The Deepfake regulatory Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power to acquire, hold and dispose of property, both movable and immovable, and to contract, and shall by the said name sue and be sued.

- (3) The head office of Deepfake regulatory Authority shall be at New Delhi and may, with the prior approval of the Central Government, establish offices at other places in India.

#### 4. Composition of authority

- (a) a Chairperson, who shall be an eminent person having adequate knowledge, expertise and experience in the matters pertaining to AI, digital media, technology, cybersecurity, content regulation to be appointed by the central government;
- (b) six ex officio members to be appointed by the Central Government, representing the Ministries dealing with—
  - (i) Electronics and Information technology;
  - (ii) Law and justice;
  - (iii) Information broadcasting;
  - (iv) External affairs;
  - (v) Science and technology;
  - (vi) Any other ministry as central government may notify from time to time;
- (c) three representatives from State Governments, nominated on a rotational basis possessing relevant expertise or experience in governance, technology regulation, or community outreach;
- (d) Five non-official members to be appointed from amongst experts including technologist, data protection specialist, psychologists and representatives of NGO'S having special knowledge or matters in relating to ethical use of AI, deepfakes and prevention of digital harm.
- (e) a Member-Secretary, who shall be a person with experience in administration, digital governance, or regulatory affairs, to be appointed by the Central Government, and who shall be responsible for day-to-day functioning, coordination, and implementation of the Authority's directives.

#### 5. Qualifications for appointment as Chairman, Vice-Chairman and other Members. — (1) A person shall not be qualified for appointment as the Chairman unless he is, or has been

- (a) has held a position in a regulatory capacity with expertise in information technology law, privacy law, or media regulation; or
- (b) has, for at least five years, served as a senior policy-maker or administrator in a relevant field such as artificial intelligence governance, data protection, cybersecurity, or digital media regulation

Provided that a person appointed as Vice-Chairman before the commencement of this Act shall be qualified for appointment as Chairman if such person has held the office of Vice-Chairman for at least two years and possesses substantial experience in technology policy or regulatory oversight.

#### (2) A person shall not be qualified for appointment, —

- (a) as an Administrative Member, unless he or she has held for at least two years the post of Secretary or Additional Secretary in a Ministry or Department dealing with Information Technology, Information & Broadcasting, or any other field directly relevant to digital governance, or has equivalent experience in managing regulatory, compliance, or enforcement frameworks at the national or international level
- (b) as a technical member unless he or she has at least five years, held the post of Additional Secretary or equivalent in departments handling legal affairs, technology regulation, or data protection, or in telecom departments

- (3) The Chairman, vice-chairman and every other Member shall be appointed by the President of India on the recommendation of a Selection Committee constituted by the Central Government, after consulting
  - (a) Chief justice of India
  - (b) At least two eminent persons having expertise in artificial intelligence, digital ethics or synthetic media governance
- (4) The chairman, vice- chairman and every other member shall possess significant knowledge or practical experience in one or more of the following fields, —
  - (i) Artificial intelligence or machine learning;
  - (ii) Information & broadcasting;
  - (iii) Privacy, cyber security or digital rights;
- (5) The members shall collectively represent diversity in terms of gender reflecting equitable participation.

6. **Terms of office** — (1) The Chairman, member shall hold office as such for a term of five year

Provided that no chairman, member shall hold office after he attained age of sixty-five years.

7. **Resignation and removal** — (1) The chairman, vice- chairman or any other member of the Deepfake regulatory authority may by notice in writing addressed to the central government of resigning the office:

Provided that he/she be permitted to relinquish his/her office sooner, or continue to hold office until the expiry of three months from the date of such notice or until a person is duly appointed as his replacement.

(2) The chairman, vice- chairman or any other member shall not be removed from office except by an order from the central government on the ground of proven

- (a) incapacity
- (b) been convicted of an offence involving moral turpitude
- (c) abused his position to render continuance
- (d) acquired financial interest prejudicial to his office

shall not be removed until an enquiry conducted by a judge of the supreme court and has been provided a reasonable opportunity of being heard.

8. **Salaries and allowances and other terms and conditions of service of Chairman, and other Members** (1) The salary, allowances and other terms and conditions of service of the Chairperson and other Members shall be such as may be prescribed by the central government, and shall not be varied to their disadvantage after their appointment.

9. **Powers and Functions of authority** (1) The Deepfake Regulatory Authority shall exercise and administer the following powers and functions, namely:

- a) on receiving an intimation in terms of creation, dissemination, or abuse of deepfake content violating the terms of this Act, to issue any immediate remedial or mitigation directions, and to investigate such violation and impose penalties as given in this Act;
- b) on a complaint received from any aggrieved person, including a victim of reputational harm, privacy violation, financial fraud, harassment, or psychological distress due to deepfake content, or on a requisition made by the Central Government, State Government, or any court, to investigate such complaint and impose penalties as are specified in this Act;
- c) on a complaint about non-compliance by any intermediary, platform, or service provider with consent, disclosure, or content moderation requirements under this Act, to investigate such non-compliance and impose penalties as laid down in this Act
- d) on receiving an intimation about breach of registration conditions or compliance obligations by any platform or service provider enabling creation or distribution of deepfake content, to investigate such breach and impose penalties as stipulated in this Act
- e) on a reference made by the Central Government in the case of contravention of provisions concerning misinformation, threat to national security, interference in elections, or public safety due to deepfake content, to investigate into such issues and



impose penalties as specified in this Act.

(2) The Authority can, in order to effectively discharge its functions under this Act, after having given the interested person or entity an opportunity of being heard and after making reasons in writing, issue such directions as it may deem necessary, which the interested person or entity shall be required to follow.

(3) The Authority can, on a representation made by any person or entity interested in a direction given under sub-section (1) or sub-section (2), or on a reference from the Central Government, alter, suspend, withdraw, or rescind such direction, and, in doing so, impose such terms as it may think fit, subject to which the alteration, suspension, withdrawal, or rescission shall be made.

### CHAPTER III

#### CONSENT AND DISCLOSURE FRAMEWORK

10. **Mandatory consent and disclosure framework** (1) The affected person's consent, under a case where a person's likeness, voice, identity, or personal characteristics are utilized in deepfake media, shall be unambiguous, free, specific, informed, and unconditional, gained by a clear affirmative act, and shall indicate consent to the creation, alteration, or release of such deepfake media for a particular purpose. The consent should be restricted only to such data, imagery, voice, or other personal characteristics as are essential for the purpose stated.

(2) Any portion of the consent mentioned in sub-section (1) which forms a contravention of the provisions of this Act, the rules made thereunder or any other law for the time being in force shall be void to the extent of such contravention.

(3) All requests for consent under this Act shall be made available to the Affected Person in easy and simple language, with an option to view such request in English or any language as given in the Eighth Schedule of the Constitution, and shall contain contact information of the individual or organization responsible for the receipt of queries and complaints related to consent, including a nominated officer or representative of the creator, distributor, or platform.

11. **Withdrawal of consent** (1) Where consent is the basis of the production or sharing of deepfake material, the Affected Person shall be entitled to withdraw the same at any time, and the withdrawal process shall be as simple and convenient as the process by which consent was originally provided.

(2) The withdrawal of consent, and the effects of such withdrawal, including disallowing or disabling of deepfake material, shall be at the expense of the creator or disseminator of such material, and such withdrawal shall not invalidate the legal use of the material/data taken/created prior to the withdrawal taking effect.

(3) If consent is revoked under sub-section (1), the creator, distributor, or platform shall, within a reasonable period of time, stop and direct all processors, agents, or third parties acting on their behalf to stop the creation, alteration, or sharing of the deepfake content, unless such act is otherwise authorized or required under this Act, its rules, or any other law in force.

(4) Where consent is the basis for creation or publication of deepfake material and any proceeding under this Act is in dispute, the creator, distributor, or platform will have to prove that due notice was given to the Affected Person and that consent was given in line with the provisions of this Act and its rules.

12. **Certain legitimate uses** (1) dissemination of deepfake content by an individual, platform, or organization can be permissible for lawful use:

- (a) where the deepfake content is created or used for a specific purpose with the free, voluntary, and express consent of the and where such content is only used for that purpose without any intent to harm, deceive, or mislead.
- (b) for purposes of academic research, journalism, documentary, satire, parody, or art, provided such material is properly labeled, does not deceive viewers about what it is, and is not employed for the purpose of defamatory use, impersonation, or exploitation.
- (c) for utilization by government schemes or any of its departments for deepfake technology in public awareness campaigns, emergency communications, or welfare programs, where—

- (i) the content is utilized for sending genuine information or issuing warnings during emergencies;
    - (ii) The participants have consented for their photo to be utilized in outreach or awareness activities.
  - f) for the creation of fictional or entertainment content where—
    - (i) the content is clearly identified as being synthetic;
    - (ii) no harm, fraud, defamation, or impersonation is probable or intended
  - (2) Any deepfake material created, modified, or distributed under this section shall—
    - (i) be plainly labeled declaring it to be synthetic or modified content
  - (3) The Authority may, by notification, formulate guidelines for making sure that legitimate uses of deepfake content can be separated from objectionable or deceptive usage, and compliance with this section.
13. **Disclosure obligation** (1) Anybody that creates, modifies, edits, disseminates deepfake content shall be obligated to disclose clearly that such content is digitally manipulated content
- (2) The disclosure shall include
    - (i) consent letter obtained
    - (ii) identity of the creator
    - (iii) the purpose for such creation
  - (3) Non-compliance with the disclosure requirements of this section shall be considered an offence and punishable under this Act, unless it is shown that there were reasonable efforts to comply
14. **General obligations pertaining to preservation of consent records** (1) Every person responsible for creation of deepfake content shall preserve all consent records and related communications in a secured manner.
- (2) Consent records shall be stored in a manner,
    - (i) That allows retrieval in the event of requisition, complaints and other legal proceedings
  - (3) The person obtaining consent shall protect the records from unauthorized access, alteration, destruction or tampering
  - (4) The authority shall prescribe the manner in which such records shall be stored.

## CHAPTER IV

### PROHIBITION OF MALICIOUS USES

15. **Prohibition of malicious deepfake creation** (1) Nobody shall create, produce or disseminate deepfake content with intent to cause reputational harm, harass, manipulate, defame, coerce or exploit individual, especially the vulnerable community such as celebrities and public figures.
- (2) Any person found committing malicious deepfake content shall be penalized with fines, criminal liability as prescribed by this act and any other appropriate penal laws that is in force and shall be forthwith required to remove the content.
16. **Prohibition of exploiting intimate content** (1) Nobody shall create, modify, edit, morph, share, distribute, produce or disseminate deepfake content that includes
- (i) Human private parts
  - (ii) Sexual images
  - (iii) Intimate videos
- (2) Any violation of this section shall be categorized serious offense and shall be penalized with fines, criminal liability as prescribed by this act and any other appropriate penal laws that is in force and shall be

forthwith required to remove the content and such platforms/entities shall be blocked in accordance with the rules issued by the authority under this Act until further notice.

17. **Prohibition of deepfake creation to incite violence, hatred or threaten national security** (1) No person shall create, spread, distribute or disseminate deepfake content with the intention to incite violence, escalate community hatred or threatening the sovereignty, integrity, national security of the state or affecting friendly relations with foreign states

(2) Prohibited content under this section includes

- (i) Fabrication of political speeches, political statements, opinions or using deepfake content to inflame tension against public representatives or political parties for the purpose of misleading voters or influencing elections
  - (ii) Provoking unrest or violence among certain communities
  - (iii) Circulating deepfake content aimed at undermining the defense or law enforcement operations
- (3) The authority upon receiving credible information or complaints, shall order immediate removal of such content and temporarily suspend the accounts, platforms until further notice and may initiate criminal proceedings under this act and other applicable laws

18. **Prohibition of activities relating to unlawful gain** (1) No person, entity shall create deepfake content to impersonate public figures, celebrities or individuals or any authoritative person for causing wrongful loss, for fraudulent financial gain or unlawful transaction.

(2) This prohibition applies to deepfake activities including: -

- (i) Fabricating voice message or video calls to impersonate financial officers
  - (ii) Using manipulate content to scam
- (3) Any person/ entity found responsible shall be penalized under this act and any other penal laws currently in force and restore status quo for the affected person

19. **Prohibition on distribution of deepfake content by intermediaries** (1) Intermediaries shall not knowingly facilitate the dissemination of deepfake content that is explicitly prohibited under this Act.

(2) Intermediaries shall be obligated to

- (i) Detect, filter and create reporting mechanism to prevent the spread of malicious/ prohibited deepfake content under this act.
  - (ii) Respond forthwith to notice issued by authority requiring content removal
  - (iii) Maintain records of flagged materials
- (3) Intermediaries failing to act in good faith to prevent further dissemination of such prohibited deepfake content shall be subjected to criminal liability and regulatory actions shall be taken by the authority constituted under this Act.

## CHAPTER V

### PROTECTION OF WHISTLEBLOWERS AND INFORMANTS

20. **Right to anonymity** (1) Any whistleblower or informant who reports such creation, distribution or misuse of deepfake content that has been created in violation of this Act shall have the right to anonymity through-out the investigation process or legal proceedings unless such disclosure is necessary and such disclosure shall be subjected to adequate safeguards

(2) The identity shall not be disclosed to accused or any third party.

(3) The authority shall implement secure channels for reporting, ensuring encryption preventing retaliation or harassment.

## CHAPTER VI

### RIGHTS OF VICTIMS AND REMEDIES

21. **Right to seek redressal** (1) Any individual, celebrities, public figures who are adversely affected by the spread, dissemination or distribution of malicious deepfake content, synthetic media shall have the right to seek redressal from the authority constituted under this Act, including claiming compensation for reputational harm and psychological distress caused.
- (2) The victims of such exploitation shall file complaints through available mechanisms like online platforms, helplines or grievance cells set up by the authority
- (3) The authority should give prompt help and ensure that the victims are properly informed about their rights, remedies available and process to claim compensation or legal recourse.
22. **Right to erasure of previously published deepfake content** (1) Affected person shall have the right to erasure of such manipulated content that has been uploaded that violates their privacy, dignity or reputation.
- (2) Person/ entity whoever is responsible for such publication, distribution or dissemination upon receiving notice of requestion shall take prompt action to erase the uploaded contents and shall also forthwith intimate/notify the intermediaries to remove the content from every platform within a stipulated time
23. **Remedies against platform negligence** (1) Intermediaries and platforms will be liable for negligence that facilitates or enables the distribution of malicious deepfake content, such as failure to respond to notices, response delays, or poor monitoring systems
- (2) Affected persons shall seek remedies against such negligence which encompasses financial compensation, restoration of reputation and the authority constituted under this Act may notify directives to improve content moderation and transparency
- (3) The Authority can, after investigation, impose penalties, order remedial measures, and order reporting standards to prevent recurrence and ensure future compliance.
24. **Right to appeal** (1) Any aggrieved victim of the order of the Authority, such as denial of relief, inaction, or unsatisfactory compensation, shall be entitled to appeal the order before an Appellate Tribunal appointed under this Act
- (2) The appeal shall be made within a specified period and shall state reasons for the review, documentation thereof, as well as any interim relief sought.
- (3) The Appellate Tribunal will be able to alter, affirm, or reverse decisions rendered by the Authority and give binding orders to prevent injustice and restoration of rights, subject to laws applicable.

## CHAPTER VII

### EXCEPTIONS AND SAFE HARBOR

25. **Acts not to be offences** (1) The provisions of this Act shall not apply to the creation, use, or dissemination of a deepfake where such deepfake is—
- (a) created or disseminated with the express consent of the individual so depicted;
  - (b) made for the purposes of satire, parody, caricature, or bona fide artistic expression, not amounting to obscenity, defamation, or incitement to an offence;
  - (c) made for bona fide educational, academic, journalistic, or research purposes, with adequate disclosure of its synthetic nature;
  - (d) created or used for artistic, cultural, or cinematic purposes with clear disclosure that such content is artificially generated; or
  - (e) (e) required or authorized by or under any law for the time being in force, or by any order of a court or competent authority;

Provided that the burden of proving the applicability of this section shall lie upon the person claiming the benefit thereof.

26. **Protection for acts done in good faith** (1) No person shall be liable under this Act for the creation,

publication, or use of a deepfake in good faith for the purpose of exposing corruption, maladministration, or matters of public interest, where such person has acted without malice or intent to defraud:

Provided that nothing in this section shall exempt liability for obscene deepfakes, child deepfakes, or deepfakes prejudicial to the sovereignty and security of the State.

27. **Exemption of intermediaries from liability (1)** No platform shall be held liable for any offence under this Act if it proves that—

- (i) it has observed due diligence as may be prescribed by the Central Government;
- (ii) upon receiving actual knowledge or notice from the Authority or a court of competent jurisdiction, it has expeditiously removed or disabled access to the impugned deepfake; and;
- (iii) it has maintained reasonable security practices, technical safeguards, and a grievance redressal mechanism

(2) The exemption under sub-section (1) shall not apply where the platform—

- (a) has initiated the transmission of the deepfake;
- (b) has selected the receiver of the transmission; or
- (c) has selected or modified the information contained in the transmission.

28. **Defense of due diligence (1)** Where any company or platform is charged with an offence under this Act, it shall be a valid defense if such entity proves that it had exercised due diligence and had in place adequate safeguards to prevent the commission of such offence.

## CHAPTER VIII

### TECHNOLOGICAL OBLIGATIONS AND INDUSTRY RESPONSIBILITY

29. **Obligation to watermark and disclose AI-generated content (1)** Every person, platform, or entity creating or facilitating the creation of a deepfake shall ensure that such content bears a visible or invisible watermark, digital signature, or other approved technological identifier to disclose its synthetic origin.

(2) The Central Government may, in consultation with the Authority, prescribe standards for watermarking and disclosure mechanisms.

(3) Whoever fails to comply with this section shall be punishable with fine which may extend to twenty lakh rupees, and in the case of a continuing default, with an additional fine which may extend to one lakh rupees for every day during which the default continues.

30. **Deployment of detection and labelling mechanisms (1)** Every platform which hosts, transmits, or disseminates user-generated content shall deploy reasonable and effective technological measures for the detection, identification, and labelling of deepfakes.

(2) Such platforms shall, upon detection, ensure that a clear disclaimer or label is attached to the deepfake indicating that it is artificially generated content.

(3) Failure to comply with this section shall render the platform liable to penalty not less than ten lakh rupees but which may extend to fifty lakh rupees.

31. **Maintenance of transparency reports (1)** Every platform having more than fifty lakh registered users shall publish, on a quarterly basis, a transparency report detailing—

- (a) the number of deepfake-related complaints received;
- (b) the actions taken thereon;
- (c) the average time for removal of reported content; and

- (d) details of cooperation with law enforcement agencies.
  - (2) Any person or platform failing to submit such report shall be liable to penalty not less than five lakh rupees but which may extend to twenty lakh rupees.
- 32. Responsibility of AI developers and model providers** (1) Every developer of an artificial intelligence system capable of generating deepfakes shall—
- (a) incorporate safeguards to prevent malicious misuse of such system;
  - (b) provide mechanisms for detection, traceability, and accountability; and
  - (c) maintain records of training data, testing protocols, and safety measures.
- (2) Any developer or provider who knowingly or negligently fails to comply with sub-section (1) shall be punishable with fine not less than twenty lakh rupees but which may extend to one crore rupees.
- 33. Industry codes of practice** (1) The Authority may, in consultation with industry stakeholders, frame and notify codes of practice specifying—
- (a) standards for responsible AI deployment;
  - (b) protocols for watermarking, labelling, and detection;
  - (c) safeguards against malicious or unlawful deepfake use; and
  - (d) procedures for user education and awareness.
- (2) Every platform, developer, or intermediary shall conform to such codes of practice.
- (3) Failure to comply with sub-section (2) shall render the entity liable to penalty not less than ten lakh rupees but which may extend to fifty lakh rupees.

## CHAPTER IX

### NATIONAL SECURITY AND FOREIGN INTERFERENCE

- 34. Prohibition of Foreign Deepfake Interference** (1) No foreign individual, entity, or intermediary shall create, generate, disseminate, or otherwise facilitate the dissemination of a deepfake within India, or directed at any person, institution, or system located in India, with the intent to—
- (a) influence elections or manipulate public opinion;
  - (b) threaten the sovereignty, integrity, or security of India;
  - (c) incite communal violence, public disorder, or hatred; or
  - (d) interfere with official or governmental functions.
- (2) Any person acting in contravention of sub-section (1) shall be punishable with imprisonment of either description for a term not less than five years but which may extend to ten years, and with fine not less than twenty lakh rupees.
- 35. Power to Block and Restrict Access to Harmful Content** (1) The designated Authority may, by order, direct any intermediary or platform to—
- (a) block, remove, or disable access to any deepfake deemed harmful under Section 34; and
  - (b) take preventive measures to restrict further dissemination of such deepfakes
- (2) Intermediaries failing to comply with an order under sub-section (1) shall be liable to a penalty not less than ten lakh rupees but which may extend to fifty lakh rupees
- (3) The Authority shall ensure that such blocking or restriction is proportionate, necessary, and minimally disruptive to lawful content.
- 36. Coordination with Security and Election Authorities** (1) The Authority shall coordinate with—
- (a) the Ministry of Home Affairs, intelligence agencies, and cybersecurity authorities for monitoring threats; and
  - (b) the Election Commission of India for preventing deepfake-related electoral interference.
- (2) Security and election authorities may, in consultation with the Authority, issue directions for immediate

removal of deepfakes posing imminent risks to public order, national security, or electoral integrity.

(3) Failure to comply with such directions shall render intermediaries liable under Section 35.

**37. Liability for Cross-Border Malicious Campaigns** (1) Any foreign individual, entity, or intermediary facilitating cross-border deepfake campaigns with malicious intent under Section 34 shall be liable to—

(a) criminal prosecution in accordance with Indian law;

(b) civil remedies including fines, injunctions, and compensation for damages.

(2) Any intermediary hosting, transmitting, or disseminating such content, knowing its unlawful nature, shall be deemed complicit unless it demonstrates due diligence in removal.

(3) The Authority may, in consultation with the Central Government, prescribe guidelines for detecting, tracing, and blocking such cross-border campaigns.

**38. Enhanced Punishment for Repeat Offences** (1) Any person convicted under Sections 34, 35, or 37 for a subsequent like offence shall be punishable with imprisonment of either description for a term not less than seven years but which may extend to fourteen years, and with fine not less than fifty lakh rupees.

(2) In determining the term of imprisonment or fine, the court shall consider the scale, reach, and impact of the deepfake campaign on national security, sovereignty, or public order.

**39. Extraterritorial Application** (1) The provisions of this Chapter shall apply to any offence committed outside India by any person if—

(a) the deepfake is made accessible in India; or

(b) the deepfake is directed at any individual, group, institution, or system located in India.

(2) Any person or intermediary subject to sub-section (1) shall be liable to prosecution, penalties, or remedial actions as if the offence were committed within India.

## CHAPTER X

### APPEAL AND ALTERNATE DISPUTE RESOLUTION

**40. Appeal to Appellate Tribunal** (1) Any person aggrieved by the order issued by the authority constituted under this Act may prefer an appeal to the Appellate tribunal.

(2) Every appeal referred under sub-section (1) shall be filed within a period of thirty days from the date of the order issues and shall be made in such manner as prescribed by the authority and shall be accompanied by the prescribed fee.

(3) The appellate tribunal may entertain an appeal even after a lapse of stipulated time, if it is satisfied that sufficient cause existed for not filing within the stipulated timeframe.

(4) Upon receiving the appeal, the tribunal shall provide both the parties reasonable opportunity to be heard and pass orders that it deem fit.

(5) An order passed by the Appellate Tribunal under this Act shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

**41. Alternate dispute resolution** (1) when a dispute may be resolved amicably, it may direct the parties to adopt arbitration, mediation, conciliation or any other forms of ADR mechanism

(2) The parties may mutually agree upon the proceedings for smooth settlement of the dispute.

(3) The proceedings under this section shall be confidential and any settlement reached shall be binding upon the parties.

**42. Enforcement of awards** (1) Any award rendered by arbitration under this chapter shall be enforceable



as if it were a decree of a civil court.

(2) In case of non-compliance, the authority may initiate enforcement proceedings and take such steps as may be necessary for the compliance.

## CHAPTER XI

### OFFENCES AND PENALTIES

43. **Unauthorized creation of deepfakes** (1) Whoever, without the consent of the individual so depicted, creates, generates, or otherwise produces a deepfake shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

(2) Where such deepfake is created for commercial exploitation, financial gain, or unlawful advantage, the punishment shall be imprisonment of either description for a term which may extend to five years, and with fine which may extend to ten lakh rupees

44. **Dissemination of deepfakes without consent** (1) Whoever, knowingly or having reason to believe, disseminates a deepfake without the consent of the individual so depicted shall be punishable with imprisonment of either description for a term which may extend to five years, or with fine which may extend to ten lakh rupees, or with both.

(2) Where dissemination is done through a platform having more than five lakh registered users, the punishment shall not be less than three years but may extend to seven years, and with fine not less than ten lakh rupees.

45. **Obscene and sexually explicit deepfakes** (1) Whoever creates, publishes, transmits, or causes to be transmitted any deepfake which is obscene or sexually explicit, without the consent of the individual so depicted, shall be punishable with imprisonment of either description for a term not less than three years but which may extend to seven years, and with fine not less than five lakh rupees.

(2) Where the person so depicted is a child, the punishment shall not be less than five years but may extend to ten years, and with fine not less than ten lakh rupees.

46. **Deepfakes involving children** (1) Whoever creates, disseminates, or possesses any deepfake depicting a child in an obscene, sexually explicit, abusive, or exploitative manner shall be punishable with imprisonment of either description for a term not less than five years but which may extend to ten years, and with fine not less than ten lakh rupees.

47. **Defamation and harassment by deepfakes** (1) Any person who creates or circulates a deepfake with the intention to damage, or with knowledge or reasonable belief that it is likely to damage, another person's reputation, dignity, or mental well-being, shall be liable to Imprisonment of up to three years, or a fine up to five lakh rupees, or both.

48. **Fraud, impersonation and financial offences by deepfakes** (1) Whoever, by means of a deepfake, impersonates another person with intent to—

- (a) commit fraud;
- (b) obtain property, services, or valuable security;
- (c) gain access to financial accounts, digital assets, or confidential information; or
- (d) cause wrongful loss to any person,

(2) shall be punishable with imprisonment of either description for a term not less than three years but which may extend to seven years, and with fine not less than ten lakh rupees.

(3) For the purposes of this section, impersonation by deepfake shall include voice cloning, facial manipulation, or any synthetic representation likely to cause a reasonable person to believe the impersonation to be genuine.

49. **Electoral interference through deepfakes** (1) Whoever, by means of a deepfake, publishes, transmits, or disseminates any content with intent to mislead electors, manipulate public opinion, or otherwise interfere with the free and fair conduct of elections, shall be punishable with imprisonment not less than five years but which may extend to ten years, and with fine not less than twenty lakh rupees.



50. **Deepfakes prejudicial to sovereignty and national security** (1) Whoever creates, transmits, or uses a deepfake in a manner prejudicial to the sovereignty, integrity, defence, or security of India, or to friendly relations with foreign States, shall be punishable with imprisonment for a term which may extend to life, and with fine.
- (2) Whoever conspires, abets, or attempts to commit such offence shall be liable to the same punishment as provided under sub-section (1).
51. **Malicious use against celebrities and public figures** (1) Whoever creates or disseminates a deepfake of a celebrity or public figure with intent to exploit, defraud, or commercially misappropriate the identity of such person shall be punishable with imprisonment of either description for a term which may extend to five years, or with fine which may extend to ten lakh rupees, or with both.
52. **Corporate liability for deepfake offences** (1) Where an offence under this Chapter has been committed by a company, every person who, at the time of the commission of the offence, was in charge of, and responsible to, the company for the conduct of its business, shall be deemed guilty of the offence and shall be liable to be proceeded against and punished accordingly.
- (2) Provided that nothing contained in sub-section (1) shall render any such person liable to punishment if he proves that the offence was committed without his knowledge, or that he exercised all due diligence to prevent the commission of such offence.
- (3) The company itself shall be punishable with fine not less than fifty lakh rupees but which may extend to two crore rupees.
53. **Liability of intermediaries and platforms for non-compliance** (1) Any platform which, upon receiving actual knowledge or notification from the Authority or a court of competent jurisdiction, fails to expeditiously remove or disable access to a deepfake in contravention of this Act, shall be liable to a penalty not less than ten lakh rupees but which may extend to fifty lakh rupees.
54. **Enhanced punishment for repeat offenders** (1) Whoever, having been convicted of an offence under this Chapter, is subsequently convicted of any like offence, shall be punishable with imprisonment of either description for a term not less than five years but which may extend to ten years, and with fine not less than twenty lakh rupees.
55. **Extraterritorial application of offences** (1) The provisions of this Chapter shall apply to any offence committed outside India by any person, if the deepfake so created, published, or disseminated is made accessible in India, or is directed at any individual, group, institution, or system located in India.

## CHAPTER XII

### OVERSIGHT AND REPORTING

56. **Annual Compliance Reporting** (1) Every platform, intermediary, or developer creating or facilitating the creation of deepfakes shall submit an annual compliance report to the Authority containing—

- (a) the number of deepfakes created, hosted, or disseminated;
  - (b) actions taken on complaints, notices, or orders under this Act;
  - (c) average time taken for removal or restriction of unlawful deepfakes; and
  - (d) details of cooperation with law enforcement or regulatory authorities
- (2) Any entity failing to submit the report under sub-section (1) within the prescribed period shall be liable to a penalty not less than five lakh rupees but which may extend to twenty lakh rupees.
- (3) The Authority may prescribe the format, content, and timeline for submission of such reports.

**57. Independent Audit of AI Systems** (1) Every developer or provider of artificial intelligence systems capable of generating deepfakes shall ensure an independent audit of their AI systems at least once every year, covering—

- (a) safeguards against malicious use;
  - (b) accuracy and reliability of detection mechanisms;
  - (c) security of training data and model integrity; and
  - (d) compliance with transparency, watermarking, and disclosure obligations under this Act.
- (2) The audit shall be conducted by an accredited independent agency approved by the Authority.
- (3) Non-compliance with sub-section (1) shall render the entity liable to a penalty not less than twenty lakh rupees but which may extend to one crore rupees.

**58. Establishment of Transparency Portal** (1) The Authority shall establish and maintain a publicly accessible transparency portal containing—

- (a) aggregate data on complaints, actions taken, and removal of deepfakes;
  - (b) quarterly and annual compliance reports submitted by intermediaries, platforms, and developers;
  - (c) advisories, guidelines, and codes of practice issued under this Act.
- (2) Entities required to submit reports under Section 76 shall ensure that relevant information is uploaded on the portal in a timely and accurate manner.
- (3) Any entity failing to comply with sub-section (2) shall be liable to a penalty not less than five lakh rupees but which may extend to twenty lakh rupees.

**59. Parliamentary Oversight and Reporting** (1) The Authority shall prepare an annual report on the implementation of this Act, including—

- (a) number and nature of offences detected and investigated;
  - (b) enforcement actions, penalties imposed, and prosecutions initiated;
  - (c) effectiveness of technological safeguards, watermarking, and labelling; and
  - (d) recommendations for legislative or policy improvements.
- (2) The annual report shall be submitted to the Central Government, which shall place it before both Houses of Parliament.
- (3) The Authority may also provide supplementary reports to Parliament or its committees as may be required for oversight purposes

## CHAPTER X

### MISCELLANEOUS

**60. Power of Central Government to issue directions** (1) The Central Government may, for the purposes of carrying out the provisions of this Act, issue to—

- (a) any authority or body established under this Act;
  - (b) any intermediary, platform, or service provider regulated under this Act;
  - (c) any person engaged in the creation, distribution, or hosting of digital content—
  - (d) such directions as it may consider necessary in respect of technological, operational, or compliance obligations.
- (2) Without prejudice to the generality of sub-section (1), such directions may relate to—
- (a) adoption of specified technological safeguards against deepfake creation and dissemination;
  - (b) preservation and furnishing of information or data relevant to enforcement of this Act;
  - (c) restriction or blocking of access to harmful deepfake content;
  - (d) adherence to prescribed industry codes or standards of practice.
- (3) Every person or entity to whom a direction is issued under this section shall be bound to comply with such direction, and non-compliance shall be deemed a contravention under this Act.
- (4) No direction under this section shall be issued except for reasons to be recorded in writing.

**61. Consistency with other laws** (1) The provisions of this Act shall be in addition to, and not in derogation of, the provisions of any other law for the time being in force. Provided that, in the event of any inconsistency between the provisions of this Act and the provisions of any other law, the provisions of this Act shall prevail to the extent of such

inconsistency.

(2) Nothing contained in this Act shall affect—

- (a) the operation of the Information Technology Act, 2000, insofar as it relates to offences, intermediaries, and cyber security;
- (b) the operation of any law relating to copyright, defamation, obscenity, or electoral integrity;
- (c) the powers of courts or other authorities under any other enactment;

21 of 2000

**62. Power to make rules retrospectively** (1) The Central Government may, by notification in the Official Gazette, make rules for carrying out the provisions of this Act.

(2) Without prejudice to the generality of sub-section (1), such rules may provide for—

- (a) the classification of offences under this Act and penalties thereof;
- (b) obligations of intermediaries and platforms, including due diligence, reporting, and cooperation with authorities;
- (c) industry codes of practice for responsible development and deployment of artificial intelligence systems;
- (d) standards for independent audits and annual reporting;
- (e) procedures for blocking, restricting, or removing deepfake content.

(3) The rules made under this section may be given retrospective effect from a date not earlier than the date of commencement of this Act.

(4) Every rule made under this section shall be laid before each House of Parliament, and shall be subject to modification, annulment, or approval in the manner provided by law.

LOK SABHA

---

A

BILL

*To protect individuals, celebrities, companies and institutions from the from the adverse social, economic, psychological and privacy-related impacts of deepfakes; to regulate the creation of deepfake across technological platforms; to establish deepfake regulation authority for oversight and to function as grievance redressal mechanism; to promote ethical and responsible use of Artificial intelligence and related technologies; to protect national security against the threats posed by deepfakes and protect sovereignty and security of the state and to provide remedies to victims of such harmful usage of deepfake technology ; to establish a uniform, national-level legal framework in the public interest; and for matters connected therewith or incidental thereto.*

---