ARTIFICIAL INTELLIGENCE TECHNOLOGY (CRIME PREVENTION AND REGULATION) BILL, 2025

ARRANGEMENT OF SECTIONS

CHAPTER I

PRELIMINARY

SECTIONS

CHAPTER II

OFFENCES & PUNISHMENT

CHAPTER VII

DATA GOVERNANCE AND SECURITY PROTOCOLS

CHAPTER VIII

RIGHTS AND DUTIES OF DEPLOYERS

CHAPTER IX

ACCOUNTABILITY

CHAPTER X

MISCELLANEOUS

ARTIFICIAL INTELLIGENCE TECHNOLOGY (CRIME PREVENTION AND REGULATION) BILL, 2025

BILL NO. OF 2025

An Act to provide for the effective regulation and oversight of the artificial intelligence systems by developing a robust legal enforcement model to address the challenges of AI-enabled crimes and to prevent and mitigate the AI- related offenses, thereby protecting the fundamental rights of citizens. The said act aims to establish accountability and liability to developers, deployers and users of artificial intelligence systems, to further amend the Bharatiya Nyaya Sanhita, the Bharatiya Saksha Adhiniyam, 2023 the Digital Personal Data Protection Act, 2023and the Information Technology Act, (Amendment) 2008, and to provide for the establishment of Tribunal for the trial of such offenses under the said Act.

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

CHAPTER I

PRELIMINARY

1.Short title, extent, and commencement. – (1) This Act may be called the Artificial Intelligence Technology Regulation Act, 2025

(2) It extends to the whole of India. , including the territorial waters, airspace and to persons on ships and aircrafts registered in India wherever they may be.

(3) It shall also apply to—

(a) any offence committed outside India by any person which has an effect on, or threatens the security or interests of India;

(b) companies or bodies corporate incorporated under any law in India;

(c) citizens of India outside India.

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

2. Definitions. – In this Act, unless the context otherwise requires,-

(1) “AI” means artificial intelligence;

(2) “artificial intelligence” means an artificial system designed to act rationally, including an intelligent software agent or embodies machine-based system, for a given set of human-defined objectives, making predications, recommendations or decisions influencing real or virtual environments, using perception, planning, reasoning, learning, communicating, decision making and acting;

(3) “autonomous AI” means an artificial intelligence system having the capability to make independent decisions and taking actions to achieve goals without simultaneous human intervention;

(4) “algorithm” means a set of rules or a computational procedure that is typically used to solve a specific problem;

(a) “algorithmic bias” means systematic and unfair discrimination that results from the design and application of algorithms, often leading to unjust outcomes in decision making processes;

(5) “biometric data” means personal data from specific technical processing relating to the physical, physiological, or behavioural characteristics of a person, such as facial images, fingerprint, eye sensor;

(a) “biometric identification” means the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a person through biometric data of that person;

(b) “biometric verification” means the automated, one-to-one verification, including authentication, of the identity of persons by comparing their biometric data to previously provided biometric data;

(6) “cloning” means creation of a digital replica of voice, likeliness, or personality of any person using artificial intelligence system.

(7) “cybercrime” means an unlawful act committed using a computer, network, artificial intelligence or internet as the tool, target, or both;

(8) “cyberstalking” means the use of artificial intelligence system, internet or digital tools to harass, threaten, or stalk someone;

(10) “data” means recorded information, regardless of form or the media on which the data is recorded;

(11) “data theft” means an unauthorised acquisition of digital data from an entity;

(12) “deepfake” means a form of audio-visual content that has been generated or manipulated using artificial intelligence that misrepresents someone or something;

(13) “developer” means a natural or legal person, public authority, agency, or other body that develops an artificial intelligence system or a general model or that has an artificial intelligence system or a general-purpose model developed and places it on the market or puts the artificial system into service under its own name or trademark, whether for payment or free of charge;

(14) “deployer” means a natural or legal person, public authority, agency, other body using artificial intelligence system under its authority except where the system is used for personal non-professional activity;

(15) “hacking” means unauthorised access to computer material;

(16) “impersonation” means an act of falsely representing oneself as another person, or a person who does not exist, with the intent to deceive or cheat;

(17) “internet” means the global network or interconnected computer and telecommunications facilities that transmit information using the Transmission Control

Protocol/ Internet Protocol or successor protocols. It encompasses the entire system of connected computer networks worldwide, allowing for global communication and data exchange;

(18) "machine learning" means an application of artificial intelligence that is characterized by providing system the ability to automatically learn and improve based on data or experience, without being explicitly programmed;

(19) "malware" means a software designed to destroy, damage, disable, or gain unauthorised access to any artificial intelligence system, computer system, software, or electronic data;

(20) "morph" means a deepfake technology of artificial intelligence system used to manipulate images or videos to create a new, often false depiction;

(21) "neural network" means a type of artificial intelligence and machine learning system, similar to the human brain, having the ability to recognise the patterns in data to perform complex tasks and procedures;

(22) "sabotage" means wilfully and intentionally damage, destroy or making defective of any material, premises, or utilities using artificial intelligence system or AI tools.

(23) "special public prosecutor" means a public prosecutor specified as special public prosecutor or an advocate referred to section of Chapter V of the Act;

(24) "tribunal" means tribunal constituted under section of Chapter V to try the offences under this Act;

CHAPTER II

OFFENCES & PUNISHMENT

3. AI-Generated Obscene and Intimate Material. - (1) Whoever creates, produces or generates using artificial intelligence system of –

(a) any sexually explicit images, videos, or audio content of any woman without her consent;
(b) morphed, manipulated, or fabricated explicit content by superimposing a woman's face onto another person's body;
(c) uses woman's photographs, videos or audio for the creation of pornographic content,

shall be punishable with imprisonment for a term of three years, which may extend to seven years and with a fine of two lakh rupees which may extend to ten lakh rupees.

4. Distribution of AI-Generated Intimate Material. – Whoever distributes, produces, transmits through any medium of the content described in section 3, shall be punishable for a term of five years, which may extend to ten years and with a fine of two lakh rupees which may extend to ten lakh rupees.

5. AI-Enabled Sexual Harassment and Stalking. – Whoever uses the artificial intelligence systems to send AI- generated sexually explicit images, videos or audio content, or create AI chatbots programmed to sexually harass, or uses AI-generated stalking tool to track, monitor or predict woman's behaviour or movements, or generate AI voiced to impersonate others for

sexual harassment shall be punishable for a term of one year which may extend to three years and with a fine of five lakh rupees, which may extend to ten lakh rupees.

6. AI- Generated Child Sexual Abuse Material. – Whoever, creates, produces, or generates using artificial intelligence system of –

(a) any sexually explicit images, videos, or audio content of any child;
(b) depicting children as adults in any pornographic material;
(c) create pseudo-photographs, videos or audio of child sexual abuse material;
(d) morph, manipulate or superimpose a child's face onto sexually explicit material or content,

shall be punished with rigorous imprisonment for a term of ten years which may extend to imprisonment for life and with a fine of ten lakh rupees, which may extend to twenty lakh rupees.

7. Distribution of AI- Generated Child Sexual Abuse Material. - Whoever distributes, produces, transmits through any medium of the content described in section 6, shall be punished with the same punishment as prescribed in section 6 of the Act.

8. AI-Generated Child Grooming and Exploitation. – Whoever uses artificial intelligence system to create chatbots, or tools to-

(a) groom, lure, entice children for sexual exploitation;
(b) create child-friendly AI personas, characters, or tools for sexually abusing children;
(c) creates false social media accounts or online characters using artificial intelligence system, or tool for predatory purposes;
(d) analyse children's behavioural patterns for sexual exploitation;
(e) create deepfake content for grooming or exploitation of children;
(f) facilitate child trafficking through AI systems or tools;

shall be punishable with rigorous imprisonment for a term not less than seven years, which may extend to imprisonment for life and with a fine of twenty lakh rupees.

9. Punishment for Storage of AI-Generated Child Pornographic Material. – Whoever, keeps storage of child pornographic material in the form of images, videos, audio, AI-chatbots, system or tools, shall be punishable with rigorous imprisonment for a term not less than ten years, which may extend to twenty years and with a fine of ten lakh rupees.

10. AI-Voice Cloning for Intimate Material. – Whoever creates, produces, or distributes AI-voice cloning of any woman or child having sexually explicit content, shall be punishable with imprisonment for a term not less the five years, which may extend to seven years and with a fine of five lakh rupees.

11. Deepfake Material. – (1) Whoever creates, produces, distributes, or transmits deepfake material using artificial intelligence system, machine learning, neural networks with a malicious intention to –

(a) defame or damage the reputation of any person;
(b) abuse or harass any person;
(c) deceive others about the identity, statements, or actions of any person;
(d) cause emotional distress, anxiety, or psychological harm;

(e) obtain wrongful gain or cause wrongful loss;

shall be punishable with imprisonment for a term of three years and with a fine of one lakh rupees.

(2) Whoever commits the offence under sub-section (1) against public servant shall be punishable with imprisonment for a term of five years and with a fine of fifty-thousand rupees.

12. Political and Electoral Deepfake Manipulation. – Whoever uses deepfake technology of artificial intelligence system to create, produce, distribute, or transmit with malicious intent to-

(a) impersonate political candidates, leaders, or public official;
(b) fabricate speeches, statements, or endorsements by political figures;
(c) spread false information to influence electoral processes or public opinion;
(d) depict public or political figures for illegal or compromising activities;
(e) manipulate democratic processes using AI-generated disinformation;

shall be punishable for a term of two years, which may extend to five years and with a fine of not less than three lakh rupees.

13. Unauthorized AI- Surveillance and Espionage. – (1) Whoever uses artificial intelligence and machine learning system for unauthorized surveillance or espionage activities to –

(a) deploy AI- enabled spyware or software for monitoring without consent;
(b) analyse the intercepted communications or data;
(c) carry out automated corporate or industrial espionage;
(d) use AI tools for unauthorized tracking, profiling, monitoring, or behavioural analysis;
(e) conduct illegal surveillance using facial recognition or biometric AI systems;

shall be punishable with imprisonment for a term of two years, which may extend to three years and with a fine of fifty-thousand rupees, which may extend to one lakh rupees.

(2) Whoever conducts espionage under sub-section (1) which involves national security, defence secrets or critical infrastructure information, shall be punishable with imprisonment or a term of ten years, which may extend to imprisonment for life.

14. Deepfake Evidence Tampering. – Whoever creates or modifies digital evidence using deepfake technology of artificial intelligence system, or submits fabricated evidence as genuine evidence in any tribunal, court, or legal proceeding, or fabricates testimony, pleadings, confessions or documentary evidence using artificial intelligence system, or uses deepfake technology of artificial intelligence system to obstruct justice, or sabotages, conceals, or alter the evidence using deepfake technology of artificial intelligence system, shall be punishable with imprisonment for a term of three years, which may extend to seven years and with fine of fifty-thousand rupees.

15. Forgery. – Whoever uses artificial intelligence system for forging documents, digital signature, counterfeiting of documents, fake identity documents, certificates, academic degrees, professional licenses or any other official records shall be punishable with

imprisonment for a term of three years, which extend to five years and with a fine of fifty-thousand rupees.

16. Automated Data Theft. – (1) Whoever uses artificial intelligence system to –

(a) steal, copy or extract personal data, financial information, confidential information of any person;
(b) use AI system to identify and target valuable data for theft;
(c) use stolen data to perpetuate further criminal activities;

shall be punishable with imprisonment for a term of three years, which may extend to five years and with a fine of five lakh rupees.

(2) If the data stolen under sub-section (1) containing biometric data, medical records, personal information of more than one thousand persons, or classified government records, trade secrets, diplomatic ties, or personal data of children and women, shall be punishable with imprisonment for a term of five years which may extend to imprisonment for life and with a fine.

17. Hacking and Phishing. – Whoever uses artificial intelligence system, machine learning algorithms, or AI tools to-

(a) gain unauthorized access to any computer system, network, or digital infrastructure;
(b) breach security protocols, firewalls, or access control using AI system
(c) bypass authentication systems or security measures;
(d) create phishing campaigns to mimic communications;
(e) deploy AI chatbots or voice synthesis for conducting phishing attacks targeting any person, corporate organisations, or government;

shall be punishable with imprisonment for a term which may extend to three years and with a fine of three lakh rupees.

18. Malicious AI Software and Computer Viruses. – Whoever creates, develops, distributes, or deploys –

(a) self-learning malware that adapts to security measures using AI system to destroy the computer system;
(b) malware or other computer viruses which uses machine learning to evade detection and hide their presence which can cause maximum damage;

shall be punishable with imprisonment for a term not more than two years and with a fine.

19. Automated Financial Fraud. – (1) Whoever uses artificial intelligence system to steal financial information of any person, conduct fraudulent financial transactions, bypass biometric security system of computer using AI tools, or conduct automated credit card fraud, banking fraud, or insurance fraud, shall be punishable with imprisonment for a term which may extend to five years and with a fine.

(2) Whoever uses artificial intelligence system to operate fraudulent investment scheme, create false trading algorithm or investment platforms, generate false financial reports or data,

target any person for financial fraud schemes, shall be punishable for a term not less than five years and with a fine of which may extend to five lakh rupees.

20. AI- Facilitated Terrorism and Unlawful Activities. - (1) Whoever uses artificial intelligence system to plan, coordinate, execute terrorist activities, recruit individuals for terrorist organisations, spread terrorist ideology, or incite violence using artificial intelligence system, provide aid or financial funds digitally through AI platforms or services, train or instruct others to conduct terrorist activities shall be punishable with imprisonment for life, which may extend to sentencing to death penalty.

(2) Whoever uses artificial intelligence system to destroy, disrupt, or damage critical infrastructure of the state, compromise national defence system, military installations, or security networks, target nuclear facilities, chemical plants, or other hazardous infrastructure using AI systems, shall be punishable with imprisonment for life.

21. AI- Generated Disinformation. – (1) Whoever, creates or distributes AI- generated content with the intent to –

(a) undermine the national security, sovereignty, or territorial integrity;
(b) incite communal violence, riots, or disrupt public order and safety;
(c) spread panic, perpetuate divisions in the state based on caste, creed, or religion during the national emergencies;
(d) damage India's relations with foreign countries or international organisations;

shall be punishable with imprisonment for life.

(2) If such disinformation results in loss of more than one-thousand lives, shall be punishable with imprisonment for life, which may extend to sentencing to death penalty.

22. AI-enabled Weaponisation. – Whoever develops, manufactures, deploys or uses autonomous weapons to cause bodily harm, injury or death, for conducting criminal or terrorist activities, AI- enhanced weapons with the capability of causing mass causalities shall be punishable with imprisonment for life or death.

23. Systematic Algorithmic Discrimination. – (1) Whoever knowingly creates, develops, deploys, or operates artificial intelligence system that discriminates against any person or a group based on race, caste, creed, religion, gender, disability, age, socio-economic status, nationality, region, domicile –

(a) in the services of employment by systematic exclusion;
(b) perpetuate biases in hiring, promotion, or performance evaluation in the services of employment;
(c) deny equal opportunities through biased algorithmic decision making;
(d) deny privileges from government services or schemes;
(e) falsely accuses a person of crime;

shall be punishable for a term of imprisonment which may extend to three years an with a fine of five lakh rupees.

24. Attempt, Abetment, and Conspiracy. - (1) Whoever attempts to commit or abets or conspires to commit any offence under this Act shall be punished with the punishment provided for the offence.

(2) For the purposes of this section, conspiracy shall include any agreement to develop, train, or deploy an AI system for the commission of an offence under this Act.

25. Prohibition of Banned AI Applications. - (1) No person shall manufacture, import, distribute, sell, or otherwise make available any banned AI application specified in Schedule I.

(2) Whoever contravenes sub-section (1) shall be punishable with imprisonment which may extend to seven years and with fine.

26. Enhanced punishment for repeat offenders. – Whoever, having been convicted of an offence under this Act, is again convicted of the same offence, shall be punishable with double the term of imprisonment and double the amount of fine provided for such offence.

CHAPTER III

REGULATORY AND OVERSIGHT

27. Establishment of the National Artificial Intelligence Security Authority. - (1) The Central Government shall, by notification, establish an Authority to be known as the National Artificial Intelligence Security Authority (hereinafter referred to as "the Authority").

(2) The Authority shall consist of a Chairperson and such number of Members, not exceeding nine, as may be prescribed, having special knowledge of artificial intelligence, information technology, national security, law, ethics, and cyber forensics.

(3) The Chairperson and Members shall be appointed by the Central Government in such manner and for such term as may be prescribed.

(4) The Authority shall be a body corporate 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.

28.Powers and functions of the Authority. - (1) The Authority shall—
(a) advise the Central Government on policies relating to the regulation of artificial intelligence systems;

(b) issue directions to intermediaries, service providers, and AI developers to prevent misuse of AI;
(c) maintain a National Register of Prohibited and High-Risk AI Systems;
(d) conduct audits and inspections of AI systems;
(e) frame guidelines for ethical use of AI;
(f) coordinate with law enforcement agencies for enforcement of this Act;
(g) undertake awareness, training and capacity-building programmes;
(h) submit annual reports to the Central Government.

29. Power to prohibit use of certain AI systems. - (1) Where the Central Government or the Authority is satisfied that the operation of any AI system poses a threat to the sovereignty and integrity of India, security of the State, friendly relations with foreign States, or public order, it may, by order published in the Official Gazette, prohibit the use, operation, or dissemination of such AI system.

(2) Every such order shall be laid before each House of Parliament.

30. Extraterritorial application.- (1) The provisions of this Act shall apply to—
(a) any person who commits an offence under this Act outside India, if the act or its effect is felt within India;
(b) any AI system deployed outside India but accessible within India;
(c) any citizen of India or company incorporated in India, wherever located.
(2) For the purposes of investigation and trial, the person may be dealt with in the same manner as if the offence had been committed within India.

31. Protection of sensitive data. - (1) No person shall train, deploy or operate any AI system on datasets containing sensitive personal data without the prior approval of the Authority.
(2) Any contravention of this section shall be punishable with imprisonment which may extend to five years, or with fine which may extend to one crore rupees, or with both.

32. Confidentiality. - (1) All proceedings, information and materials obtained under this Act shall be treated as confidential, except where disclosure is required by a Court of law or by rules made under this Act.
(2) Whoever contravenes this section shall be punishable with imprisonment up to three years, or fine up to ten lakh rupees, or with both.

33. Power of Central Government to issue directions. - (1) The Central Government may, in the interest of sovereignty and integrity of India, national security, or public order, issue to the Authority or to any person such directions as it may deem necessary.

(2) Every person to whom such direction is issued shall be bound to comply with the same

34. Power of Central and State Government to aid implementation. - The State Government shall take all such measures as may be necessary to give effect to the provisions of this Act and shall cooperate with the Authority in enforcement thereof.

35. Offences by companies. - (1) Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed, was in charge of and responsible for the conduct of the business of the company shall be deemed guilty of the offence.

(2) Nothing contained in this section 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 the offence.

(3) Where an offence under this Act has been committed by a company and it is proved that the offence was committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such person shall be deemed guilty of the offence.

CHAPTER IV
INVESTIGATIVE AND PROCEDURAL FRAMEWORK

36. Cognizable and non-bailable offences. - Notwithstanding anything contained in the Bharatiya Nagarika Suraksha Sanhita, 2023—
(a) every offence under this Act shall be deemed to be a cognizable and non-bailable offence;
(b) the provisions of the BNSS shall apply, subject to the provisions of this Act.

37. Designated Authority for investigation. - (1) The Central Government may, by notification, designate such authority or agency of the Central Government as it may deem fit for the investigation of offences under this Act.
(2) The State Government may, with the concurrence of the Central Government, designate such authority or agency of the State Government for investigation within the State.
(3) No officer below the rank of Deputy Superintendent of Police or equivalent shall investigate any offence under this Act.

38. Powers of investigation. - (1) Any officer authorised under section 17 may—
(a) enter, search and seize any premises, equipment, storage device, server or cloud resource suspected to be used for the commission of an offence under this Act;

(b) arrest, without warrant, any person suspected of having committed an offence under this Act;

(c) require the disclosure of decryption keys, access credentials, or any other assistance necessary for accessing AI systems;

(d) take possession of, or assume control over, any AI system, data, or model;

(e) require any intermediary, service provider, or data centre to furnish information or provide technical assistance.

(2) The provisions of the BNSS, relating to search, seizure and arrest shall apply, subject to the provisions of this Act.

39. Admissibility of electronic and AI-generated evidence. - (1) Notwithstanding anything contained in the Indian Evidence Act, 1872, any record, log, output, or decision trace generated by an AI system shall be admissible in evidence if accompanied by a certificate of authenticity issued by a designated forensic authority.
(2) The Court may, for the purposes of evidence, presume the accuracy of any AI-generated output unless proved otherwise by the accused.

40. Custody and preservation of seized AI systems. - (1) Where any AI system, model, or dataset is seized under this Act, the investigating officer shall ensure its secure preservation in accordance with such standards as may be prescribed.
(2) The Central Government shall establish Digital Evidence Management Centres for the storage and preservation of seized AI models and data.
(3) The Court may order the forfeiture or destruction of such AI systems if found to be unlawful.

41. Interception and monitoring. - (1) Where the Central Government or the State Government is satisfied that it is necessary so to do in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order, it may

direct any agency—
(a) to intercept, monitor or decrypt any communication transmitted or generated using an AI system;
(b) to collect metadata, training logs, or usage patterns of any AI system.
(2) The procedure, safeguards, and duration for interception shall be such as may be prescribed, consistent with the directions of the Supreme Court.

42. Bail. - (1) No person accused of an offence punishable with imprisonment of seven years or more under this Act shall be released on bail or on his own bond unless—
(a) the Public Prosecutor has been given an opportunity to oppose the application; and
(b) where the Public Prosecutor opposes the application, the Court is satisfied that there are reasonable grounds for believing that the accused is not guilty and is not likely to commit any offence while on bail.
(2) The restrictions under sub-section (1) are in addition to the restrictions under the Bharatiya Nagarika Suraksha Sanhita, 2023.

43. Attachment and forfeiture of property. - (1) Where any person is accused of an offence under this Act, the investigating officer may, with the prior approval of the Court, attach any property believed to be derived from the proceeds of such offence.
(2) The Court may, on conviction, order the forfeiture of such property.
(3) The provisions of the Prevention of Money Laundering Act, 2002, shall apply, mutatis mutandis, to attachment and forfeiture under this Act.

44. Protection of witnesses and victims. - (1) The Court may take such measures as it deems necessary for keeping the identity and address of any witness or victim secret.
(2) No person shall print or publish in any matter the name, address, photograph, or any other particulars calculated to lead to the identification of a witness or victim.
(3) Whoever contravenes sub-section (2) shall be punishable with imprisonment which may extend to three years and with fine.

CHAPTER V

TRIBUNAL

45. Establishment of Tribunal. - (1) The Central Government shall, by notification in the Official Gazette, establish a Tribunal, to be known as the Artificial Intelligence Tribunal ,hereinafter referred to as the Tribunal, to exercise the jurisdiction, powers, and authority conferred on it by or under this Act.

(2) The Tribunal shall consist of a Presiding Officer and such number of Judicial Members and Technical Members as the Central Government may deem fit.

(3) The establishment of the Tribunal shall be for the purpose of ensuring a fair, efficient, and specialized adjudication of offences related to Artificial Intelligence, including but not limited to, criminal liability arising from autonomous systems, data manipulation, and algorithmic biases.

46. Composition and Qualification of Members. - (1) The Presiding Officer of the Tribunal shall be a person who is or has been a Judge of a High Court, as per the provisions of the Constitution of India.

(2) A Judicial Member shall be a person who is who is or has been a Sessions Judge or an Additional Sessions Judge under the Bharatiya Nagarik Suraksha Sanhita, 2023.

(3) A Technical Member shall be a person having special knowledge of, and professional experience in, the fields of Artificial Intelligence, machine learning, data science, cybersecurity, or computer engineering, with at least ten years of experience in the relevant field.

(4) No person shall be appointed as a Presiding Officer or Judicial Member unless they have attained the age of fifty years.

47. Benches of the Tribunal. - (1) The powers and functions of the Tribunal may be exercised by Benches thereof.

(2) A Bench shall ordinarily consist of one Judicial Member and one Technical Member.

(3) In cases involving grave offences punishable with imprisonment for a term of seven years or more, or in any matter of significant public importance as notified by the Central Government, the Bench shall consist of the Presiding Officer, one Judicial Member, and one Technical Member.

48. Special Public Prosecutor. - (1) For every Tribunal, the Central Government shall, in consultation with the Presiding Officer, appoint a person to be a Special Public Prosecutor.

(2) A person shall be eligible to be appointed as a Special Public Prosecutor only if they have been in practice as an advocate for not less than twenty years and have special knowledge of AI technologies and cyber-crime.

(3) The Special Public Prosecutor shall conduct all prosecutions before the Tribunal and shall be deemed to be a Public Prosecutor within the meaning of the Bharatiya Nagarik Suraksha Sanhita, 2023.

49. Territorial Divisions. - (1) The Central Government shall, by notification, determine the territorial jurisdiction of each Tribunal.

(2) The Tribunal may hold its sittings at such places within its territorial jurisdiction as the Presiding Officer may, from time to time, direct.

50. Exclusive Jurisdiction of the Tribunal. - (1) Notwithstanding anything contained in the Bharatiya Nagarik Suraksha Sanhita, 2023, or any other law for the time being in force, the Tribunal alone shall have the jurisdiction to inquire into, try, and adjudicate upon any offence specified under this Act.

(2) No Court, other than the Tribunal, shall have the jurisdiction to entertain any application, suit, or proceeding in respect of any matter which is by or under this Act required to be dealt with by the Tribunal.

(3) Any proceeding pending before any Court in respect of an offence under this Act on the date of its commencement shall, upon such commencement, stand transferred to the Tribunal having jurisdiction.

51. Powers and Procedure of the Tribunal. - (1) The Tribunal shall have the same powers as are vested in a Court of Session under the Bharatiya Nagarik Suraksha Sanhita, 2023, for the trial of offences.

(2) Without prejudice to the generality of the foregoing, the Tribunal shall have the power to:

(a) issue summons for the attendance of any person and examine them on oath;
(b) require the discovery and production of documents and electronic records;
(c) receive evidence on affidavits;
(d) issue commissions for the examination of witnesses or documents;
(e) review its own decisions or orders;
(f) issue directions for the attachment and forfeiture of property related to the commission of the offence.

(3) In all criminal proceedings before it, the Tribunal shall be guided by the principles of natural justice and the provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023.

52. Penalties and Orders. - (1) The Tribunal may, upon finding an accused person guilty of an offence under this Act, impose such penalty as is prescribed for that offence, including imprisonment, fines, or both.

(2) The Tribunal may, in addition to any penalty, pass an order for:

(a) the deactivation or removal of the harmful AI system;
(b) the forfeiture of any gain or property obtained through the commission of the offence;
(c) compensation to the victim;
(d) an order to the accused to perform community service.

53. Appeal to the High Court. - Any person aggrieved by an order or decision of the Tribunal may prefer an appeal to the High Court within whose jurisdiction the Tribunal is situated, within a period of sixty days from the date of communication of the order or decision.

54. Application of Bharatiya Sakshya Adhiniyam, 2023. - (1) The provisions of the Bharatiya Sakshya Adhiniyam, 2023, shall apply to all proceedings before the Tribunal.

(2) The Tribunal shall specifically have the power to admit and evaluate electronic and digital evidence, including code, algorithms, and data logs, as per the provisions of the said Adhiniyam.

(3) For the purpose of securing digital evidence, the Tribunal may, in accordance with the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Bharatiya Sakshya Adhiniyam, 2023, order the seizure of any electronic device, server, or cloud data storage.

55. Special Powers of the Tribunal. - (1) The Tribunal may, upon application by the Special Public Prosecutor, issue directions to any person or entity to provide any information, including confidential source code or proprietary data, necessary for the investigation or trial of an offence under this Act.

(2) The Tribunal may, for reasons to be recorded in writing, allow for a trial to be held in-camera where the subject matter involves sensitive technology or national security.

56. Other Provisions. - All matters not expressly provided for in this Act shall be governed by the provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023, in so far as they are not inconsistent with the provisions of this Act.

CHAPTER VI

CLASSIFICATION AND ASSESSMENT

57. Classification and Assessment. - (1) For the purposes of this Act, Artificial Intelligence systems (hereinafter referred to as "AI systems") shall be classified based on their potential to cause significant harm to individuals, groups, or public safety and security.

(2) The classification shall be a mandatory prerequisite for the deployment of any AI system.

(3) The Regulatory Authority established under Chapter III shall be the sole authority responsible for the classification, assessment, and oversight of AI systems as per the provisions of this chapter.

58. Categories of AI Systems. - AI systems shall be classified into the following categories:

(1) Prohibited AI Systems, hereinafter referred to as Prohibited AI, whose applications are deemed to be an inherent threat to fundamental rights, public order, and safety, and are strictly banned;

(2) High-Risk AI Systems, hereinafter referred to as High-Risk AI, which have the potential to cause significant harm to individuals or society, and are subject to stringent penal and regulatory requirements;

(3) Limited-Risk AI Systems, hereinafter referred to as Limited-Risk AI, which pose minimal or no risk and are subject to minimal regulatory oversight;

59. Prohibited AI. - Any AI system designed or used for the following purposes shall be classified as a Prohibited AI, if -

(1) the use of subliminal techniques can materially distort a person's behaviour in a manner that causes or is likely to cause physical or psychological harm;

(2) the creation of automated social scoring systems that evaluate or classify the trustworthiness of individuals based on their social behaviour;

(3) any system intended to deploy autonomous weapons that are not under meaningful human control;

(4) any system designed to commit offenses under the Bharatiya Nyaya Sanhita, 2023 without human intervention;

(5) the deepfake technology, or any other machine learning tool of the AI system is used for committing any of the offences as mentioned in Chapter II of the Act;

(6) the AI system is used for unauthorized surveillance or carrying out espionage;

(7) the AI system is capable of sabotaging critical infrastructure;

(8) the AI system is used for developing or deploying autonomous weapons;

60. High-Risk AI. - An AI system shall be classified as a High-Risk AI if it is intended to be used in any of the following fields:

(a) Law Enforcement and Criminal Justice: AI systems used for predictive policing, bail risk assessments, facial recognition for surveillance, or forensic analysis;
(b) Critical Infrastructure: AI systems used for the management or control of electricity grids, water supply, transportation networks, or other essential services.
(c) Employment and Education: AI systems used for automated recruitment, resume shortlisting, or the grading and evaluation of students.
(d) Healthcare: AI systems used for medical diagnosis, drug discovery, or surgical procedures.
(e) (2) Every High-Risk AI system must undergo a mandatory and rigorous Fundamental Rights Impact Assessment to evaluate its potential for bias, discrimination, and violation of the principles enshrined in the Constitution of India.

(3) The Regulatory Authority shall, in accordance with the Bharatiya Sakshya Adhiniyam, 2023, have the power to demand access to the source code, training data, and any other electronic record necessary for this assessment.

61. Penalties for Misclassification and Non-Compliance. - (1) Any person or entity that intentionally provides false information or misclassifies an AI system to circumvent the provisions of this Act shall be guilty of an offense and punished with imprisonment for a term of seven years, which may extend to ten years and with a fine of five lakh rupees.

(2) The offense of misclassification shall be considered a cognizable and non-bailable offense under the Bharatiya Nagarik Suraksha Sanhita, 2023, and the Regulatory Authority shall have the power to initiate criminal proceedings.

(3) Failure to comply with any assessment or audit order issued by the Regulatory Authority shall be punishable with a fine of up to ten crore rupees, in addition to any other penalties specified under this Act.

CHAPTER VII

DATA GOVERNANCE AND SECURITY PROTOCOLS

62. Data classification and sensitivity levels. – (1) The Authority shall prescribe standards for classification of data used in training, testing, and deployment of AI systems, into the following categories: —

(a) public data;

(b) sensitive personal data;

(c) critical infrastructure data;

(d) national security data.

(2) Any AI developer or deployer shall handle such data strictly in accordance with the classification guidelines.

63. Storage and retention protocols. - (1) Every person handling AI datasets shall maintain secure servers in India for storage of sensitive personal data and national security data.

(2) The maximum period for retention of training datasets shall be prescribed by regulations, subject to necessity and proportionality.

64. Audit of datasets and models. - (1) The Authority may direct periodic audit of datasets and models used by high-risk AI systems.

(2) Such audits shall ensure compliance with standards of accuracy, fairness, bias mitigation, and privacy.

65. Data-sharing restrictions. - (1) No person shall transfer or permit transfer of critical infrastructure data or national security data outside India without prior approval of the Central Government.

(2) Any contravention shall be punishable with imprisonment which may extend to seven years, and with fine.

66. Incident reporting and breach notification. – (1) Any person or entity deploying AI systems shall mandatorily report to the Authority within seventy-two hours of any data breach, cyber-attack, or compromise of AI models.

(2) Failure to comply shall attract penalty which may extend to rupees one crore, in addition to liability for damages.

67. Encryption and access control. - (1) Every high-risk AI system shall deploy state-of-the-art encryption and access-control protocols as may be prescribed.

(2) Decryption keys shall be provided to the Authority upon lawful request for investigation.

68. Protection of personal data in AI training. – (1) No AI system shall use personal data for training purposes unless—

(a) consent of the data principal has been obtained;

(b) the data has been lawfully anonymised and aggregated.

69. Cross-sectoral coordination. - The Authority shall coordinate with the Data Protection Board established under law, CERT-In, and other agencies to ensure consistent enforcement of data governance norms.

70. Penalties for non-compliance. – (1) Whoever contravenes any provision of this Part shall be punishable with imprisonment which may extend to five years, or with fine which may extend to rupees two crore, or with both.

(2) Where the contravention is by a company, the company as well as persons responsible shall be liable.

CHAPTER VIII

RIGHTS AND DUTIES OF DEPLOYERS

71. Duty of registration and compliance. - (1) Every deployer of a high-risk AI system shall register such system with the Authority before use.

(2) Every deployer shall comply with the conditions of licence, standards of safety, and directions issued by the Authority.

72. Duty of transparency. - (1) A deployer shall ensure that the operation of high-risk AI systems is transparent, explainable and documented in such manner as may be prescribed.

(2) A deployer shall maintain records of training datasets, algorithms and decisions made by the AI system for a minimum period of five years.

73. Duty of accountability. - (1) A deployer shall be responsible for any unlawful act committed by its AI system unless he proves that all due diligence was exercised to prevent such act. (2) A deployer shall designate an officer responsible for compliance with this Act.

74. Right to lawful deployment. - Every registered deployer shall have the right to deploy AI systems for lawful purposes without undue interference, subject to compliance with this Act and rules made thereunder.

75. Right to appeal. - Every deployer aggrieved by an order of the Authority refusing or revoking registration or imposing penalties shall have the right to prefer an appeal before the AI Security Appellate Tribunal.

76. Duty to prevent misuse. – A deployer shall take reasonable steps, including technical safeguards and human oversight, to prevent the misuse of AI systems under its control for terrorist or unlawful activities.

77. Duty to cooperate with investigations. – A deployer shall extend all reasonable assistance to investigating agencies or the Authority in matters relating to offences under this Act.

78. Confidentiality and protection of proprietary rights. – (1) Nothing in this Act shall be construed to require disclosure of proprietary algorithms, trade secrets or intellectual property, except to the extent strictly necessary for investigation or regulatory compliance.

(2) The Authority shall protect confidential information obtained from deployers and shall not disclose it except in the interests of national security or by order of a competent court.

79. Duty to educate and train users. - Every deployer of a high-risk AI system shall provide adequate information, training, and warnings to users regarding potential risks, limitations, and safeguards of the system.

CHAPTER IX

ACCOUNTABILITY

80. Principle of accountability. - Every authority, deployer, developer, and intermediary governed by this Act shall be accountable for compliance with its provisions and for ensuring that artificial intelligence systems are not misused for terrorist or unlawful purposes.

81. Vicarious liability of organisations. - (1) Where an offence under this Act is committed by a company, society, or association, every person who, at the time the offence was committed, was in charge of and responsible for the conduct of its business shall be deemed guilty of the offence.

(2) No person shall be liable under this section if he proves that the offence was committed without his knowledge and that he exercised all due diligence to prevent its commission.

82. Liability of government officials. – (1) Any officer of the Authority or of the Government who knowingly abuses his powers under this Act or acts with mala fide intent shall be liable to disciplinary action and penalties as may be prescribed.

(2) No prosecution shall be instituted against such officer without the sanction of the Central Government.

83. Independent oversight. - (1) The Comptroller and Auditor General of India shall have the power to audit the functioning of the Authority, including its accounts, processes, and exercise of powers.

(2) An annual report on compliance and accountability under this Act shall be laid before both Houses of Parliament.

84. Whistleblower protection. – (1) Any person who, in good faith, makes a disclosure of misuse, abuse of power, or non-compliance under this Act shall be protected from civil or criminal liability.

(2) The identity of such whistleblower shall be kept confidential, except as may be required by law.

85. Personal liability of officers of deployers. – (1) Where a deployer fails to comply with the obligations under this Act, the designated compliance officer shall be personally liable for such failure.

(2) Penalties under this section shall not be imposed where the officer proves that due diligence and reasonable safeguards were exercised.

86. Review and accountability framework. - (1) The Central Government shall, every three years, constitute a committee to review the operation of this Act and to recommend measures for strengthening accountability.

(2) The report of such committee shall be made public, except portions relating to national security.

CHAPTER X

MISCELLANEOUS

87. Power to Make Rules. - (1) The Central Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters: (a) The form and manner in which an application shall be made to the Regulatory Authority under Section 35(2). (b) The procedure for conducting the Fundamental Rights Impact Assessment and the criteria for its evaluation. (c) The manner of imposing penalties, including the procedure for the payment of fines and the recovery of compensation. (d) Any other matter which is required to be, or may be, prescribed.

88. Protection of Action Taken in Good Faith. - No suit, prosecution, or other legal proceeding shall lie against the Regulatory Authority or any officer or other employee of the

Central Government or the State Government for anything which is in good faith done or intended to be done in pursuance of this Act or any rule made thereunder.

89. Overriding Effect. - The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force or in any instrument having effect by virtue of any law other than this Act.

90. Removal of Difficulties. - (1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty.

(2) Every order made under this section shall, as soon as may be after it is made, be laid before each House of Parliament.

91. Act not to affect lawful research. - Nothing in this Act shall apply to bona fide research and development activities in artificial intelligence undertaken by recognised academic institutions, unless such research is used for unlawful purposes.

92. Repeal and Savings. - (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.

(2) Notwithstanding such repeal, anything done or any action taken under any enactment so repealed shall be deemed to have been done or taken under the corresponding provisions of this Act.

SCHEDULE I

High-Risk Artificial Intelligence Systems (refer to section 59 of Chapter

1. Generative models capable of producing deepfakes.
2. Autonomous decision-making systems in critical infrastructure.
3. AI systems capable of simulating biometric or personal data.
4. Military-grade autonomous weapons using AI.
5. AI systems trained on sensitive personal or classified datasets.
6. Deepfake technology used for committing any of the offences under the Chapter VI.
7. Designed to commit offenses under the Bharatiya Nyaya Sanhita, 2023 without human intervention.
8. Unauthorized Surveillance and Espionage.
9.

STATEMENT OF OBJECTS AND REASONS

The rapid growth of Artificial Intelligence (AI) technologies has created unprecedented opportunities and challenges for the Republic of India. While AI has the potential to accelerate innovation, productivity, and social welfare, it equally poses grave threats when deployed for unlawful purposes, including deepfakes, disinformation, cyber-attacks, and autonomous weapons. At present, there exists no comprehensive legislation in India addressing the misuse of AI in matters concerning national security, public order, sovereignty and integrity of the State. Existing enactments such as the Unlawful Activities (Prevention) Act, 1967, the Information Technology Act, 2000, and the Indian Penal Code, 1860, provide

only partial safeguards and do not adequately cover the unique risks of AI systems. In the absence of a clear statutory framework, malicious actors are increasingly exploiting AI systems to mislead the public, destabilise democratic processes, and endanger critical infrastructure. There is also a risk of cross-border deployment of hostile AI models targeting India's sovereignty and integrity. This Bill, therefore, seeks to—

1. Define and criminalise specific categories of unlawful activities relating to AI, including creation of harmful deepfakes, AI-enabled terrorist activities, and misuse of AI in critical infrastructure.
2. Establish an investigative and procedural framework for regulating AI systems, including search, seizure, admissibility of AI-generated evidence, and establishment of Special Courts.
3. Create the National Artificial Intelligence Security Authority to regulate, monitor, and issue directions concerning high-risk and prohibited AI systems.
4. Provide for extraterritorial jurisdiction, protection of sensitive data, and overriding effect over inconsistent laws.
5. Ensure that lawful academic research and innovation in AI remain unaffected while safeguarding the sovereignty, integrity, and security of the State.

The Bill is designed in harmony with constitutional principles, balancing the need for innovation with the imperative of national security.

FINANCIAL MEMORANDUM

Clause 28 of the Bill provides for the establishment of the National Artificial Intelligence Security Authority. The Authority will require expenditure from the Consolidated Fund of India. The estimated recurring expenditure will include salaries and allowances of the Chairperson and Members, staff salaries, infrastructure costs for Digital Evidence Management Centres, and maintenance of the National Register of Prohibited AI Systems. In the initial year, the expenditure is estimated to be approximately **₹250 crore**, covering establishment of the Authority, creation of Digital Evidence Management Centres in five zones, and recruitment of technical experts. The recurring annual expenditure is estimated to be approximately **₹150 crore**, subject to revision depending on operational requirements and expansion of regulatory infrastructure. No provision of the Bill is likely to cause recurring expenditure beyond the amounts specified, other than that incidental to enforcement by law enforcement agencies.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 39 of the Bill empowers the Central Government to make rules for carrying out the purposes of the Act. The matters in respect of which such rules may be made are matters of detail which are not practicable to provide in the Bill itself. The delegation of legislative power is, therefore, of a normal character.