

AS INTRODUCED IN THE RAJYA SABHA
ON THE 5TH DECEMBER, 2025

Bill No. XLV of 2025

THE CLASSIFIED INFORMATION AND ESPIONAGE
CONTROL BILL, 2025

A
BILL

*to establish a comprehensive legal framework for the classification,
protection and management of sensitive information relating to
national security; to regulate the authorised access, handling
and disclosure of such information; to penalise
unauthorised access and disclosure, including
acts of espionage; to safeguard constitutional
rights and ensure transparency; and to repeal
the Official Secrets Act, 1923, along with
matters connected therewith or
incidental thereto.*

WHEREAS it is expedient to provide a comprehensive and contemporary legislative framework for the classification and protection of sensitive information pertaining to the sovereignty, integrity, defence and strategic interests of India;

AND WHEREAS it is necessary to criminalise espionage and unlawful disclosures while safeguarding the right to information, whistleblower protection and democratic oversight.

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

CHAPTER I

PRELIMINARY

Short title,
application and
commencement.

1. (1) This Act may be called the Classified Information and Espionage Control Act, 2025. 5
- (2) The provisions of this Act shall apply to,—
- (a) every citizen of India, whether within or outside the territory of India;
- (b) any person on board a ship or aircrafts registered in India, wherever they may be; and 10
- (c) any person, irrespective of citizenship, whether within or beyond the territorial boundaries of India, who unlawfully obtains or discloses classified information concerning the national interest of India and thereby commits an offence under this Act. 15
- (3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint, and different dates may be appointed for different provisions of this Act.

Definitions.

2. In this Act, unless the context otherwise requires—
- (a) “Board” for the purpose of this Act is Independent Review Board on National Security and Disclosures, established under section 11; 20
- (b) “classified information” means any information, document, material or communication declared by the Central or State Government to be sensitive to national security, defence or strategic interests, and marked confidential, secret or top secret, the unauthorised disclosure of which is likely to prejudice national security or international relations; 25
- Explanation.*— For the purpose of this clause, “unauthorized disclosure” means dissemination of classified information by a person who is not authorised or who acts in violation of this Act. 30
- (c) “espionage” means any act of accessing, obtaining, recording, copying, disclosing, transmitting or retaining classified information with the intent to harm the sovereignty, integrity or security of India; 35
- (d) “information” means any oral, written, electronic or any other form of communication or data, whether tangible or intangible, and whether stored, transmitted or received by any means;
- (e) “public interest disclosure” means disclosure made in good faith to an authorised constitutional authority for exposing corruption, illegality or abuse of power; and 40
- (f) “prescribed” means prescribed under the rules made under this Act.

CHAPTER II

CLASSIFICATION AND HANDLING OF INFORMATION

Classification
Protocol.

3. (1) The Central Government shall, by notification in the official Gazette, establish a system for classification of information based on sensitivity, and such system shall include levels of category such as “Confidential”, “Secret” and “Top Secret” or such other levels as may be notified from time to time. 50

(2) The classification referred to in sub-section (1), shall be based on the sensitivity, potential harm to national security, and duration for which secrecy is warranted in the interest of the state.

5 (3) No classification shall be made or maintained with the intent to conceal corruption, abuse of authority, or violations of human rights.

4. (1) All information classified under section 3, shall be subject to periodic review by the Board, constituted under section 12, at an interval not exceeding five years from the date of such classification or of the last review, as the case may be.

Declassification
and Review.

10 (2) Notwithstanding anything contained in sub-section (1), the Board referred to in sub-section (1), on its own motion or on the recommendation of any such authority or person as may be prescribed, may declassify any information at any time prior to the expiry of the period specified therein, if it is satisfied that disclosure of such
15 information no longer prejudices national security.

5. (1) No person shall be granted access to any information classified under the provisions of this Act, except where such person is holding a valid security clearance, issued by such authority and after following due clearances as may be prescribed.

Security
clearance and
need-to-know
access.

20 (2) Information shall be shared strictly on a need-to-know basis, and any unauthorised access or attempt to obtain such information without lawful authority shall be a punishable offence under this Act.

CHAPTER III

OFFENCES AND PENALTIES

25 6. (1) A person shall be deemed to have committed the offence of espionage, if such person with wilful intent or purpose prejudicial to the sovereignty, integrity, security, or strategic interests of the State,—

Espionage.

30 (a) approaches, inspects, photographs, records, surveys, geolocates, flies drones over, or enters any prohibited place, sensitive digital network, secured defence installation, or protected perimeter, without lawful authority; or

35 (b) makes, copies, transmits, digitises, hacks, decrypts, models, or otherwise generates any sketch, plan, schematic, model, map, topographic data, digital representation, or other record, in any form, physical or digital, which is calculated to be, or is likely to be, or is intended to be, directly or indirectly useful to a foreign power, non-state actor, or enemy entity; or

40 (c) obtains, collects, mines, leaks, records, sells, trades, or communicates, whether directly or indirectly, through artificial intelligence systems, spyware, hacking, data scrapers, bots, or digital surveillance tools; any secret official password, classified document, data set, protocol, communication, intelligence, model, program, code, algorithm, or information, which,—

45 (i) is likely to be, or is intended to be, directly or indirectly useful to an enemy or a foreign power; or

(ii) relates to a matter the disclosure of which is likely to affect the sovereignty and integrity of India, the security of the State, defence preparedness, critical infrastructure, or friendly relations with foreign States.

50 (2) Any person found guilty of the offence of espionage under sub-section (1) shall be punished with imprisonment for a term not less than ten years, which may extend to life imprisonment, or with fine upto one crore rupees or with both.

Presumption of
prejudicial
purpose.

7. In a prosecution under section 6, it shall not be necessary to prove that the accused committed a specific act with prejudicial intent, and the Court may presume such intent if:—

(a) the accused was found in possession of any classified material without lawful authority;

5

(b) the act occurred in or involved a prohibited area or critical information infrastructure;

(c) the nature of the information and the circumstances suggest use or potential use by foreign powers, hostile entities, or unlawful groups; or

10

(d) the accused's past conduct, known affiliations, or use of clandestine or anonymised digital tools indicate malicious intent.

Explanation 1.— For the purposes of this section,—

(a) "enemy" includes any country, organisation, individual, or non-state actor engaged in hostile actions or intelligence operations against India; and

15

(b) "prohibited place" includes any area, building, data centre, server room, airspace, territorial zone, military base, or digital network declared restricted or classified as such by the Central Government.

20

Explanation 2.— Mere unauthorised possession, access, or communication of classified content—whether physical, digital, or algorithmic—without lawful justification or authority shall constitute a violation under this section.

Possession of
classified
material
without
authority.

8. (1) Whoever, without lawful authority, is found in possession of any classified information, document, model, article, data, record or material, whether in physical, electronic, or any other form, which is marked or deemed to be classified under the provisions of this Act or the rules made thereunder, shall be punished with imprisonment for a term which may extend to five years, or with fine which may extend to ten lakh rupees, or with both.

25

30

(2) It shall not be a defence under this section that the accused was not aware of the classified nature of the information, unless it is proved that such possession was accidental, without intent, and without any failure to exercise due diligence.

35

(3) Nothing in this section shall apply to any person who makes a bona fide disclosure in public interest to a designated authority in accordance with the provisions of this Act.

Attempts,
conspiracy and
abetment.

9. Any person who attempts to commit, conspires to commit, or abets any offence under this Act shall be deemed to have committed the offence and punished with the same penalties for the said offence under this Act.

40

Offences by
companies.

10. (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 to the company for the conduct of its business shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

45

Provided that nothing in this sub-section shall render any such person liable to any punishment provided in this Act, if he proves that the contravention or offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such contravention or offence.

50

(2) Notwithstanding anything contained in sub-section (1), where a contravention or an offence under this Act has been committed by a

company and it is proved that the contravention or offence was committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary, or any other officer of the company, such person shall also be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Explanation.— For the purposes of this section,—

(a) "company" means anybody corporate and includes a co-operative society registered or deemed to be registered under any law for the time being in force, a firm or other association of individuals; and

(b) "director", in relation to a firm, means a partner in the firm.

CHAPTER IV

PUBLIC INTEREST AND OVERSIGHT

11. (1) Notwithstanding anything contained in this Act, no person shall be liable to prosecution or any form of penal action under this Act for making a disclosure, in good faith and in the larger public interest, of any classified information to a designated authority.

Public interest disclosure and whistleblower protection.

(2) A disclosure under sub-section (1) shall be entitled to protection under this section only if,—

(a) it is supported by reasonable grounds and verifiable evidence;

(b) it is made in writing or through such secure and verifiable means as may be prescribed;

(c) it is made only to a designated authority, as notified by the Central Government in the official Gazette, including but not limited to the Supreme Court, High Courts, Lokpal, or the Comptroller and Auditor General of India; and

(d) it is not disclosed to any unauthorised person, media outlet, foreign entity, or digital platform prior to the completion of formal review by the designated authority or the Board.

(3) The Board constituted under section 12 shall, upon receipt of a reference from a designated authority, examine whether such disclosure qualifies for protection under this section and shall communicate its decision within a period of ninety days from the date of such reference.

Explanation.— For the purposes of this section, "good faith" shall mean an honest belief held with due care and reasonable diligence; and "public interest" shall include the exposure of corruption, abuse of power, gross mismanagement, or serious threats to public health, safety, or democratic accountability.

12. (1) The Central Government shall, by notification in the official Gazette, establish a body to be known as the Independent Review Board on National Security and Disclosures for the purposes of this Act.

Establishment of the Independent Review Board on National Security and Disclosures.

(2) The Board shall consist of the following members, to be appointed by the Central Government in such manner as may be prescribed, namely—

(a) a retired Judge of the Supreme Court or a retired Chief Justice of a High Court, who shall be the Chairperson;

(b) one senior officer, who retired from not below the rank of Secretary to the Government of India, with experience in defence, intelligence, or national security — Member;

Laying of
reports.

Grants by the
Central
Government.

- (c) one expert in cybersecurity, information warfare, or digital data protection — Member; and
- (d) one person of eminence in the field of constitutional law, civil liberties, or public accountability — Member.
- (3) The term of office, salaries and/or allowances payable to, and other terms and conditions of service of, the Chairperson and Members of the Board shall be such as may be prescribed. 5
- (4) The Board shall have the following powers and functions, namely—
- (a) to receive and review references from designated authorities regarding disclosures made under section 11 of this Act; 10
- (b) to determine whether such disclosures qualify for protection as public interest disclosures under section 11;
- (c) to recommend classification or declassification of information in accordance with national security and democratic transparency; 15
- (d) to issue guidance to public authorities on classification, retention, and dissemination of sensitive material;
- (e) to investigate into complaints regarding violation of the provisions of this Act and hear appeals from individuals aggrieved by decisions of competent authorities under this Act; 20
- (f) to prepare and submit annual reports on its activities and findings to the Central Government; and
- (g) any other function related to the subject, as may be assigned to it by the Central Government.
- (5) The Board shall regulate its own procedure and while investigating any matter under clause (e) of sub-section (3) have all the powers of a civil court under the Code of Civil Procedure, 1908, while trying a suit in respect of the following matters, namely— 25 5 of 1908.
- (a) summoning and enforcing the attendance of any person and examining him on oath; 30
- (b) requiring the discovery and production of documents;
- (c) receiving evidence on affidavits; and
- (d) issuing commissions for the examination of witnesses or documents.
- (6) The decisions of the Board shall be binding on all public authorities and shall not be called in question in any court except by way of a petition under article 226 of the Constitution before the High Court having jurisdiction. 35
- (7) The Central Government may appoint such number of officers and staff to the Board, as it deems necessary, to assist it in the efficient discharge of its functions under this Act. 40
- (8) The method of appointment, salaries and allowances payable to, and the other terms and conditions of service of the Chairperson, Members, officers and other employees, so appointed for the purpose of the Board shall be such as may be prescribed. 45
13. The Central Government shall cause the reports of the Board under clause (f) of sub-section (4) of section 12 to be laid before each House of Parliament, as soon as may be after they are received.
14. The Central Government, after due appropriation made by Parliament by law in this behalf, pay to the Board by way of grants 50

such sums of money as it may consider necessary for carrying out the purposes of this Act.

15. (1) The Board shall, in consultation with the Comptroller and Auditor-General of India, maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form and manner and at such time of each financial year or at such intervals, as may be prescribed.
- (2) The accounts of the Board shall be audited by the Comptroller and Auditor-General or by any person appointed by him in this behalf at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Board to the Comptroller and Auditor-General.
- (3) The accounts of the Board, as certified by the Comptroller and Auditor-General or any other person appointed by him in this behalf, together with the audit report thereon shall be forwarded annually by the Board to the Central Government, which shall cause it to be laid, as soon as may be after it is received, before each House of Parliament.

Accounts and audit.

CHAPTER V

PROCEDURE, JURISDICTION, AND MISCELLANEOUS

16. (1) Offences under this Act shall be cognizable and non-bailable.
- (2) No investigation of any offence under this Act shall be initiated without the prior approval of a Joint Secretary-level officer in the Government of India.
17. (1) Notwithstanding anything contained in the Bharatiya Nagarik Suraksha Sanhita, 2023, all offences punishable under this Act shall be triable only by a Sessions Court, specially designated by the Central Government for the said purpose, by notification in the Official Gazette.
- (2) Proceedings or any part thereof may be held by the Court in camera, if it is satisfied that it is expedient so to do in the interest of national security.
18. This Act shall apply to any person outside India who commits an offence under this Act affecting the security of India, and such person shall be dealt with in accordance with the provisions of this Act.
19. (1) The Central Government may, by notification in the Official Gazette, make rules to carry out the purposes of this Act, including classification, review procedure, whistleblower protocols, and reporting.
- (2) The Board may, with the prior approval of the Central Government, by notification in the Official Gazette, make regulations not inconsistent with the provisions of this Act and the rules made thereunder, to provide for all matters for which provision is necessary or expedient for the purposes of giving effect to the provisions of this Act.
- (3) Every rule made by the Central Government and every regulation made by the Board under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

Cognizance and investigation.

Jurisdiction and trial.

Extraterritorial jurisdiction.

Power of Central Government to make rules and of the Board to make regulations.

20. (1) The Official Secrets Act, 1923 is hereby repealed.

Repeal and Savings.

(2) Notwithstanding such repeal, anything done or any action taken, including any investigation, inquiry, prosecution or legal proceeding commenced under the said Act, shall, in so far as it is not inconsistent with the provisions of this Act, be deemed to have been done or taken under the corresponding provisions of this Act as if this Act were in force at the time such act or action was done or taken. 5

Act to override other laws.

21. The provisions of this Act shall prevail over any other law for the time being in force, in the case of any inconsistency therewith, save as to such laws which relate to the enforcement of rights guaranteed under Part III of the Constitution. 10

Power to remove difficulties.

22. (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:

Provided that no such orders shall be made after the expiry of the period of two years from the date of commencement of this Act. 15

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

STATEMENT OF OBJECTS AND REASONS

The Second Administrative Reforms Commission, in its 2006 report, recommended that secrecy provisions be integrated into a broader national security framework that is consistent with democratic accountability, constitutional safeguards, and transparency obligations. The rise of cyber-espionage, AI-enabled surveillance, data leaks, and emerging threats to critical infrastructure underscores the urgency of a robust legal mechanism to protect India's strategic interests.

The Official Secrets Act, 1923, a colonial-era law, has been long criticised for its vague provisions and alleged incompatibility with democratic norms. Its proposed repeal is a necessary reform to clearly address the issue of unauthorised access, communication or retention of classified information related to national security, defence, and intelligence. In the absence of a modern legal framework, the State remains exposed to espionage, cyber-infiltration, and digital breaches in an era of transnational data flows and growing threats from foreign powers and non-state actors.

This Bill seeks to establish a comprehensive and rights-compatible legal framework for the classification and protection of sensitive information. It clearly defines key terms such as espionage, unauthorised disclosure, and public interest disclosure, and criminalises the use of modern technological means, such as hacking, spyware, and surveillance tools for espionage. It safeguards whistleblowers acting in good faith by exempting disclosures made to designated authorities. The Bill also establishes an Independent Review Board on National Security and Disclosures to oversee the classification decisions and protect whistleblower rights. Harmonised with the existing laws including the Right to Information Act, 2005, the Whistle Blowers Protection Act, 2014, and the Digital Personal Data Protection Act, 2023, this Bill proposes to repeal the Official Secrets Act, 1923 and replace it with a modern and constitutionally sound regime that balances national security with democratic accountability.

Hence, this Bill.

SUJEET KUMAR.

FINANCIAL MEMORANDUM

Clause 12 of the Bill provides for the establishment of an Independent Review Board on National Security and Disclosures, its composition, the appointment of officers and staff by the Central Government to assist the Board as well as for the salaries and allowances payable to and the other terms and conditions of service of the Chairperson, Members, officers and staff thereof. Clause 14 of the Bill empowers the Central Government to make grants to the Board, after due appropriation made by Parliament in this behalf, for the purposes of carrying out the provisions of the Act.

The Bill, therefore, if enacted, would involve expenditure from the Consolidated Fund of India. It is estimated that a recurring expenditure of about rupees one crore would be incurred per annum from the Consolidated Fund of India. A non-recurring expenditure of about rupees five crore is also likely to be involved.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 19 of the Bill empowers the Central Government to make rules and the Board to make regulations for carrying out the purposes of the Bill. Clause 22 of the Bill empowers the Central Government to make such provisions through an order for removing any difficulty that might arise in giving effect to the provisions of the Bill.

As the rules or regulations or orders will relate to matters of procedural and administrative detail only, the delegation of legislative power is of a normal character.

RAJYA SABHA

A

BILL

to establish a comprehensive legal framework for the classification, protection and management of sensitive information relating to national security; to regulate the authorised access, handling and disclosure of such information; to penalise unauthorised access and disclosure, including acts of espionage; to safeguard constitutional rights and ensure transparency; and to repeal the Official Secrets Act, 1923, along with matters connected therewith or incidental thereto.

(Shri Sujeet Kumar, M.P.)