†O.I.H

GOVERNMENT OF INDIA

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

LOK SABHA

UNSTARRED QUESTION NO. 589

TO BE ANSWERED ON: 23.07.2025

SECTIONS RELATED TO CYBER CRIME

†589. SHRI RAKESH RATHOR:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether most of the sections relating to financial cyber crime are bailable under the Information Technology Act;

(b) if so, the details thereof;

(c) whether the Government proposes to make the crimes under the said sections nonbailable in view of the growing incidence and wider impact thereof in the country; and

(d) if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY

(SHRI JITIN PRASADA)

(a) to (d): Relevant provisions pertaining to cybercrime under the Information Technology Act, 2000 ("IT Act") and the Bharatiya Nyaya Sanhita, 2023 ("BNS") are as follows:

I. Information Technology Act, 2000 ("IT Act"):

Section 65 of the IT Act: Tampering with computer source documents.–Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.–For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Section 66 of the IT Act: Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.*Explanation*.–For the purposes of this section,–

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

Section 66B of the IT Act: Punishment for dishonestly receiving stolen computer resource or communication device.– Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C of the IT Act: Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D of the IT Act: Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E of the IT Act: Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. *Explanation*.–For the purposes of this section–

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast:

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that–

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 66F of the IT Act: Punishment for cyber terrorism.–(*1*) Whoever,–

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by–

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or

likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(*2*) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 67 of the IT Act: Punishment for publishing or transmitting obscene material in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A of the IT Act: Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B of the IT Act: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.–Whoever,–

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form–

(*i*) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(*ii*) which is kept or used for *bona fide* heritage or religious purposes.

Explanation–For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Section 69 of the IT Act: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.–(*1*) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (*2*), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (*1*), extend all facilities and technical assistance to–

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or (*c*) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in subsection (*3*) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section 69A of the IT Act: Power to issue directions for blocking for public access of any information through any computer resource.–(*1*) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (*2*), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (*1*) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Section 69B of the IT Act: Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.–(*1*) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (*1*), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (*2*) shall be punished with an imprisonment for a term which any extend to one year or shall be liable to fine which may extend to one crore rupees, or with both.

Explanation.–For the purposes of this section,–

(i) "computer contaminant" shall have the meaning assigned to it in section 43;

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data, size, duration or type of underlying service and any other information.

Section 70 of the IT Act: Protected system.– (*1*) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.–For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (*1*).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(*4*) The Central Government shall prescribe the information security practices and procedures for such protected system.

Section 70B of the IT Act: Indian Computer Emergency Response Team to serve as national agency for incident response.–(*1*) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.

(2) The Central Government shall provide the agency referred to in sub-section (*1*) with a Director General and such other officers and employees as may be prescribed.

(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.

(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security,–

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, preventation, response and reporting of cyber incidents; (*f*) such other functions relating to cyber security as may be prescribed.

(5) The manner of performing functions and duties of the agency referred to in sub-section (*1*) shall be such as may be prescribed.

(6) For carrying out the provisions of sub-section (*4*), the agency referred to in sub-section (*1*) may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person.

(7) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (*6*), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one crore rupees or with both.

(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (*1*).

Section 71 of the IT Act: Penalty for misrepresentation.–Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or electronic signature Certificate, as the case may be, shall be punished with

imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72 of the IT Act: Penalty for Breach of confidentiality and privacy.–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be liable to penalty which may extend to five lakh rupees.

Section 73 of the IT Act: Penalty for publishing electronic signature Certificate false in certain particulars.–(*1*) No person shall publish a electronic signature Certificate or otherwise make it available to any other person with the knowledge that–

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a electronic signature created prior to such suspension or revocation.

(*2*) Any person who contravenes the provisions of sub-section (*1*) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 74 of the IT Act: Publication for fraudulent purpose.–Whoever knowingly creates, publishes or otherwise makes available a electronic signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 77B of the IT Act: Offences with three years imprisonment to be bailable.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

78. Power to investigate offences.–Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [1][Inspector] shall investigate any offence under this Act.

II. Bharatiya Nyaya Sanhita, 2023 ("BNS"):

Section 111 of the BNS: Organised crime.—(*1*) Any continuing unlawful activity including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cyber-crimes, trafficking of persons, drugs, weapons or illicit goods or services, human trafficking for prostitution or ransom, by any person or a group of persons acting in concert, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate, by use of violence, threat of violence, intimidation, coercion, or by any other unlawful means to obtain direct or indirect material benefit including a financial benefit, shall constitute organised crime.

Explanation.—For the purposes of this sub-section,—

(*i*) "organised crime syndicate" means a group of two or more persons who, acting either singly or jointly, as a syndicate or gang indulge in any continuing unlawful activity;

(*ii*) "continuing unlawful activity" means an activity prohibited by law which is a cognizable offence punishable with imprisonment of three years or more, undertaken by any person, either singly or jointly, as a member of an organised crime syndicate or on behalf of such syndicate in respect of which more than one charge-sheets have been filed before a competent Court within the preceding period of ten years and that Court has taken cognizance of such offence, and includes economic offence;

(*iii*) "economic offence" includes criminal breach of trust, forgery, counterfeiting of currency-notes, bank-notes and Government stamps, *hawala* transaction, mass-marketing fraud or running any scheme to defraud several persons or doing any act in any manner with a view to defraud any bank or financial institution or any other institution or organisation for obtaining monetary benefits in any form.

(*2*) Whoever commits organised crime shall,—

(*a*) if such offence has resulted in the death of any person, be punished with death or imprisonment for life, and shall also be liable to fine which shall not be less than ten lakh rupees;

---

[1] . Subs. by Act 10 of 2009, s. 39, for "Deputy Superintendent of Police" (w.e.f. 27-10-2009).

(*b*) in any other case, be punished with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine which shall not be less than five lakh rupees.

(*3*) Whoever abets, attempts, conspires or knowingly facilitates the commission of an organised crime, or otherwise engages in any act preparatory to an organised crime, shall be punished with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine which shall not be less than five lakh rupees.

(*4*) Any person who is a member of an organised crime syndicate shall be punished with imprisonment for a term which shall not be less than five years but which may extend to imprisonment for life, and shall also be liable to fine which shall not be less than five lakh rupees.

(*5*) Whoever, intentionally, harbours or conceals any person who has committed the offence of an organised crime shall be punished with imprisonment for a term which shall not be less than three years but which may extend to imprisonment for life, and shall also be liable to fine which shall not be less than five lakh rupees:

Provided that this sub-section shall not apply to any case in which the harbour or concealment is by the spouse of the offender.

(*6*) Whoever possesses any property derived or obtained from the commission of an organised crime or proceeds of any organised crime or which has been acquired through the organised crime, shall be punishable with imprisonment for a term which shall not be less than three years but which may extend to imprisonment for life and shall also be liable to fine which shall not be less than two lakh rupees.

(*7*) If any person on behalf of a member of an organised crime syndicate is, or at any time has been in possession of movable or immovable property which he cannot satisfactorily account for, shall be punishable with imprisonment for a term which shall not be less than three years but which may extend to imprisonment for ten years and shall also be liable to fine which shall not be less than one lakh rupees.

Section 112 of the BNS: Petty organisedcrime.—(*1*) Whoever, being a member of a group or gang, either singly or jointly, commits any act of theft, snatching, cheating, unauthorised selling

of tickets, unauthorised betting or gambling, selling of public examination question papers or any other similar criminal act, is said to commit petty organised crime.

Explanation.—For the purposes of this sub-section "theft" includes trick theft, theft from vehicle, dwelling house or business premises, cargo theft, pick pocketing, theft through card skimming, shoplifting and theft of Automated Teller Machine.

(*2*) Whoever commits any petty organised crime shall be punished with imprisonment for a term which shall not be less than one year but which may extend to seven years, and shall also be liable to fine.

Section 318 of the BNS: Cheating.—(*1*) Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to cheat.

Explanation.—A dishonest concealment of facts is a deception within the meaning of this section.

(*2*) Whoever cheats shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

(*3*) Whoever cheats with the knowledge that he is likely thereby to cause wrongful loss to a person whose interest in the transaction to which the cheating relates, he was bound, either by law, or by a legal contract, to protect, shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both.

(*4*) Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

Section 319 of the BNS: Cheating by personation.—(*1*) A person is said to cheat by personation if he cheats by pretending to be some other person, or by knowingly substituting one person for or another, or representing that he or any other person is a person other than he or such other person really is.

Explanation.—The offence is committed whether the individual personated is a real or imaginary person.

Section 336 of the BNS: Forgery.—(*1*) Whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery.

(*2*) Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

(*3*) Whoever commits forgery, intending that the document or electronic record forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine.

(*4*) Whoever commits forgery, intending that the document or electronic record forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine.

Government regularly engages with citizens and stakeholders, including in respect of changes required to existing legislation and the need to introduce fresh legislation.

****