

## CRIMINAL LAW AMENDMENT ACT, 2013

### Voyeurism.

354C. Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.

Explanation 1.— For the purpose of this section, "private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy and where the victim's genitals, posterior or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the victim is doing a sexual act that is not of a kind ordinarily done in public.

Explanation 2.— Where the victim consents to the capture of the images or any act, but not to their dissemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section.

## INFORMATION TECHNOLOGY ACT (As amended in 2008)

S. 66E. Punishment for violation of privacy.— Whosoever, 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.—Fro the purposes of this section—

- (a) "transmit" means to electronically send a visual image with the internet 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;

S. 67B. 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 which 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 year 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 in 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 purpose.

Explanation—For the purpose of this section, “children” means a person who has not completed the age of 18 years.

S. 69B. 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 containment 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 may extend to three years and shall also be liable to fine.

Explanation.—For the purpose 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, date, size, duration or type of underlying service and any other information.]

72A. Punishment for disclosure of information in breach of lawful contract.—

Save as otherwise provided in this Act or any other law for the time being in force, any person including and intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine

which may extend to five lakh rupees, or with both.]

S. 84A. Modes or methods for encryption.—The Central Government may, for secure use of the electronic medium and for promotion of e-governance and ecommerce, prescribe the modes or methods for encryption.

## Guidelines For Technical and Financial Support For Establishment of State Data Centre (SDC)

### 12.0 Data Retention Plan

12.1 The State would formulate an appropriate Data Retention policy and ensure that the data centre architecture supports the same. The Data Retention Policy would be guided by the following factors:

- a. Data classification and risk assessment of data.
- b. Data Retention Period.
- c. Data Security aspects.
- d. Disposal of data once the retention period is over.

### 13.0 Data Centre Protection

13.1 The data centre shall have the required protection and safeguard mechanism for physical security, network security and facility infrastructure requirements including protection against fire, natural calamity and man made risks.

### 14.0 Security Audit

14.1 The State shall get the security audited by third party expert periodically (once in six months) and as and when there is significant upgradation of systems which include hardware, software and network resources to ensure and guarantee security of the Data Centre. The audit shall bring out any security lapses in the system and establish that the system is working as desired by the State.