The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

Notification, New Delhi, the 27th October, 2009, G.S.R. 780 (E).—In exercise of the powers conferred by clause (y) of sub-section (2) of Section 87, read with sub-section (2) of Section 69 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:

1. Short title and commencement.—(1) These rules may be called the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

(2) They shall come into force on the date of their publication in the Official Gazette.

2. Definitions.—In these rules, unless the context otherwise requires,-

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "communication" means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication;

(c) "communication link" means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource;

(d) "competent authority" means -

  (i) the Secretary in the Ministry of Home Affairs, in case of the Central Government; or

  (ii) the Secretary in charge of the Home Department, in case of a State Government or Union territory, as the case may be;

(e) "computer resource" means computer resource as defined in clause (k) of sub-section (1) of Section 2 of the Act;

(f) "decryption" means the process of conversion of information in non-intelligible form to an intelligible form via a mathematical formula, code, password or algorithm or a combination thereof;

(g) "decryption assistance" means any assistance to -

  (i) allow access, to the extent possible, to encrypted information; or

  (ii) facilitate conversion of encrypted information into an intelligible form;

(h) "decryption direction" means a direction issued under rule 3 in which a decryption key holder is directed to -

(i) disclose a decryption key; or

(ii) provide decryption assistance in respect of encrypted information

(i) "decryption key" means any key, mathematical formula, code, password, algorithm or any other data which is used to -

(i) allow access to encrypted information: or

(ii) facilitate the conversion of encrypted information into an intelligible form;

(J) "decryption key holder" means any person who deploys the decryption mechanism and who is in possession of a decryption key for purposes of subsequent decryption of encrypted information relating to direct or indirect communications;

(k) "information" means information as defined in clause (v) of sub-section (1) of Section 2 of the Act;

(l) "intercept" with its grammatical variations and cognate expressions, means the aural or other acquisition of the contents of any information through the use of any means, including an interception device, so as to make some or all of the contents of a information available to a person other than the sender or recipient or intended recipient of that communication, and includes—

(a) monitoring of any such information by means of a monitoring device;

(b) viewing, examination or inspection of the contents of any direct or indirect information; and

(c) diversion of any direct or indirect information from its intended destination to any other destination;

(m) "interception device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus! to intercept any information; and any reference to an "interception device" includes, where applicable, a reference to a "monitoring device";

(n) "intermediary" means an intermediary as defined in clause (w) of sub-section (1) of Section 2 of the Act;

(o) "monitor" with its grammatical variations and cognate expressions, includes to view or to inspect or listen to or record information by means of a monitoring device;

(p) "monitoring device" means any electronic, mechanical, electro-mechanical, electro-magnetic, optical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself in combination with any other instrument, device, equipment or apparatus, to view or to inspect or to listen to or record any information;

(q) "Review Committee" means the Review Committee constituted under rule 419A of Indian Telegraph Rules, 1951.

3. Directions for interception or monitoring or decryption of any information.—No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under sub-section (2) of Section 69 of the Act, except by an order issued by the competent authority;

Provided that in an unavoidable circumstances, such order may be issued by an officer, not below the rank of the Joint Secretary to the Government of India, who has been duly authorised by the competent authority:

Provided further that in a case of emergency-

(i) in remote areas, where obtaining of prior directions for interception or monitoring or decryption of information is not feasible; or

(ii) for operational reasons, where obtaining of prior directions for interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource is not feasible,

the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource may be carried out with the prior approval of the Head or the second senior most officer of the security and law enforcement agency (hereinafter referred to as the said security agency) at the Central level and the officer authorised in this behalf, not below the rank of the Inspector General of Police or an officer of equivalent rank, at the State or Union territory level:

Provided also that the officer, who approved such interception or monitoring or decryption of information in case of emergency, shall inform in writing to the competent authority about the emergency and of such interception or monitoring or decryption within three working days and obtain the approval of the competent authority thereon within a period of seven working days and if the approval of competent authority is not obtained within the said period of seven working days, such interception or monitoring or decryption shall cease and the information shall not be intercepted or monitored or decrypted thereafter without the prior approval of the competent authority.

4. Authorisation of agency of Government.—The competent authority may authorise an agency of the Government to intercept, monitor or decrypt information generated, transmitted, received or stored in any computer resource for the purpose specified in sub-section (1) of Section 69 of the Act.

5. Issue of decryption direction by competent authority.—The competent authority may, under rule 3 give any decryption direction to the decryption key holder for decryption of any information involving a computer resource or part thereof.

6. Interception or monitoring or decryption of information by a State beyond its jurisdiction.—Notwithstanding anything contained in rule 3, if a State Government or Union territory Administration requires any interception or monitoring or decryption of information beyond its territorial jurisdiction, the Secretary in-charge of the Home Department in that State or Union territory, as the case may be; shall make a request to the Secretary in the Ministry of Home Affairs, Government of India for issuing direction to the appropriate authority for such interception or monitoring or decryption of information.

7. Contents of direction.—Any direction issued by the competent authority under rule 3 shall contain reasons for such direction and a copy of such direction shall be forwarded to the Review Committee,, within a period of seven working days.

8. Competent authority to consider alternative means in acquiring information—The competent authority shall, before issuing any direction under rule 3, consider possibility of acquiring the necessary information by other means and the direction under rule 3 shall be issued only when it is not possible to acquire the information by any other reasonable means.

9. Direction of interception or monitoring or decryption of any specific information.—The direction of interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource shall be of any information as is sent to or from any person or class of persons or relating to any particular subject whether such information or class of information are received with one or more computer resources, or being a computer resource likely to be used for the generation, transmission, receiving, storing of information from or to one particular person or one or many set of premises, as may be specified or described in the direction.

10. Direction to specify the name and designation of the officer to whom information to be disclosed.—Every directions under rule 3 shall specify the name and designation of the officer of the authorised agency to whom the intercepted or monitored or decrypted or stored information shall be disclosed and also specify that the use of intercepted or monitored or decrypted information shall be subject to the provisions of sub-section (1) of Section 69 of the said Act.

11. Period within which direction shall remain in force.—The direction for interception or monitoring or decryption shall remain in force, unless revoked earlier, for a period not exceeding sixty days from the date of its issue and may be renewed from time to time for such period not exceeding the total period of one hundred and eighty days.

12. Authorised agency to designate nodal officer.—The agency authorised by the competent authority under rule 4 shall designate one or more nodal officer, not below the rank of Superintendent of Police or Additional Superintendent of Police or the officer of the equivalent rank, to authenticate and send the requisition conveying direction issued under rule 3 for interception or monitoring or decryption to the designated officers of the concerned intermediaries or person in-charge of computer resource:

Provided that an officer, not below the rank of Inspector of Police or officer of equivalent rank, shall deliver the requisition to the designated officer of the intermediary.

13. Intermediary to provide facilities, *etc.*—(1) The officer issuing the requisition conveying direction issued under rule 3 for interception or monitoring or decryption of information shall also make a request in writing to the designated officers of intermediary or person in-charge of computer resources, to provide all facilities, co-operation and assistance for interception or monitoring or decryption mentioned in the directions.

(2) On the receipt of request under sub-rule (1), the designated officers of intermediary or person in-charge of computer resources, shall provide all facilities, co-operation and assistance for interception or monitoring or decryption of information mentioned in the direction.

(3) Any direction of decryption of information issued under rule 3 to intermediary shall be limited to the extent the information is encrypted by the intermediary or the intermediary has control over the decryption key.

14. Intermediary to designate officers to receive and handle requisition.—Every intermediary or person in-charge of computer resource shall designate an officer to receive requisition, and another officer to handle such requisition, from the nodal officer for interception or monitoring or decryption of information generated, transmitted, received or stored in any computer resource.

15. Acknowledgement of instruction.—The designated officer of the intermediary or person in-charge of computer resources shall acknowledge the instructions received by him through letters or fax or e-mail signed with electronic signature to the nodal officer of the concerned agency within two hours on receipt of such intimation or direction for interception or monitoring or decryption of information.

16. Maintenance of records by designated officer.—The designated officer of intermediary or person in-charge of computer resource authorised to intercept or monitor or decrypt any information shall maintain proper records mentioning therein, the intercepted or monitored or decrypted information, the particulars of persons, computer resource, e-mail account, website address, *etc.* whose information has been intercepted or monitored or decrypted, the name and other particulars of the officer or the authority to whom the intercepted or monitored or decrypted information has been disclosed, the number of copies, including corresponding electronic records of the intercepted or monitored or decrypted information made and the mode or the method by which such copies, including corresponding electronic record are

made, the date of destruction of the copies, including corresponding electronic record and the duration within which the directions remain in force.

17. Decryption key holder to disclose decryption key or provide decryption assistance—If a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the nodal officer referred to in rule 12, the decryption key holder shall within the period mentioned in the decryption direction—

(a) disclose the decryption key; or

(b) provide the decryption assistance,

specified in the decryption direction to the concerned authorised person.

18. Submission of list of interception or monitoring or decryption of information—(1) The designated officers of the intermediary or person in-charge of computer resources shall forward in every fifteen days a list of interception or monitoring or decryption authorisations received by them during the preceding fortnight to the nodal officers of the agencies authorised under rule 4 for confirmation of the authenticity of such authorisations.

(2) The list referred to in sub-rule (1) shall include details, such as the reference and date of orders of the concerned competent authority including any order issued under emergency cases, date and time of receipt of such order and the date and time of implementation of such order.

19. Intermediary to ensure effective check in handling matter of interception or monitoring or decryption of information.—The intermediary or the person in-charge of the computer resource so directed under rule 3, shall provide technical assistance and the equipment including hardware, software, firmware, storage, interface and access to the equipment wherever requested by the agency authorised under rule 4 for performing interception or monitoring or decryption including for the purposes of—

(i) the installation of equipment of the agency authorised under rule 4 for the purposes of interception or monitoring or decryption or accessing stored information in accordance with directions by the nodal officer; or

(ii) the maintenance, testing or use of such equipment; or

(iii) the removal of such equipment; or

(iv) the performance of any action required for accessing of stored information under the direction issued by the competent authority under rule 3.

20. Intermediary to ensure effective check in handling matter of interception or monitoring or decryption of information.—The intermediary or person in-charge of computer resources shall put in place adequate and effective internal checks to ensure the unauthorised interception of information does not take place and extreme secrecy is maintained and utmost care and precaution shall be taken in the matter of interception or monitoring or decryption of information as it affects privacy of citizens and also that it is handled only by the designated officers of the intermediary and no other person of the intermediary or person in-charge of computer resources shall have access to such intercepted or monitored or decrypted information.

21. Responsibility of intermediary.—The intermediary or person in-charge of computer resources shall be responsible for any action of their employees also and in case of violation pertaining to maintenance of secrecy and confidentiality of information or any unauthorised interception or monitoring or decryption of information, the intermediary or person in-charge of computer resources shall be liable for any action under the relevant provisions of the laws for the time being in force.

22. Review of directions of competent authority.—The Review Committee shall meet at least once in two months and record its findings whether the directions issued under rule 3 are

in accordance with the provisions of sub-section (2) of Section 69 of the Act and where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue order for destruction of the copies, including corresponding electronic record of the intercepted or monitored or decrypted information.

23. Destruction of records of interception or monitoring or decryption of information—(1) Every record, including electronic records pertaining to such directions for interception or monitoring or decryption of information and of intercepted or monitored or decrypted information shall be destroyed by the security agency in every six months except in a case where such information is required, or likely to be required for functional requirements.

(2) Save as otherwise required for the purpose of any ongoing investigation, criminal complaint or legal proceedings, the intermediary or person in-charge of computer resources shall destroy records pertaining to directions for interception of information within a period of two months of discontinuance of the interception or monitoring or decryption of such information and in doing so they shall maintain extreme secrecy.

24. Prohibition of interception or monitoring or decryption of information without authorisation—(1) Any person who intentionally or knowingly, without authorisation under rule 3 or rule 4, intercepts or attempts to intercept, or authorises or assists any other person to intercept or attempts to intercept any information in the course of its occurrence or transmission at any place within India, shall be proceeded against and punished accordingly under the relevant provisions of the laws for the time being in force.

(2) Any interception, monitoring or decryption of information in computer resource by the employee of an intermediary or person in-charge of Computer resource or a person duly authored by the intermediary, may be undertaken in course of his duty relating to the services provided by that intermediary, if such activities are reasonably necessary for the discharge his duties as per the prevailing industry practices, in connection with the following matters, namely—

(i) installation of computer resource or any equipment to be used with computer resource; or

(ii) operation or maintenance of computer resource; or

(ii) installation of any communication link or software either at the end of the intermediary or subscriber, or installation of user account on the computer resource of intermediary and testing of the same for its functionality;

(iv) accessing stored information from computer resource relating to the installation, connection or maintenance of equipment, computer resource or a communication link or code; or

(v) accessing stored information from computer resource for the purpose of—

  (a) implementing information security practices in the computer resource;

  (b) determining any security breaches, computer contaminant or computer virus;

  (c) undertaking forensic of the concerned computer resource as a part of investigation or internal audit; or

(vi) accessing or analysing information from a computer resource for the purpose of tracing a computer resource or any person who has contravened, or is suspected of having contravened or being likely to contravene, any provision of the Act that is likely to have an adverse impact on the services provided by the intermediary.

(3) The intermediary or the person in-charge of computer resource and its employees shall maintain strict secrecy and confidentiality of information while performing the actions specified under sub-rule (2).

25. Prohibition of disclosure of intercepted or monitored or decrypted information.— (1) The contents of intercepted or monitored or stored or decrypted information shall not be used or disclosed by intermediary or any of its employees or person in-charge of computer resource to any person other than the intended recipient of the said information under rule 10.

(2) The contents of intercepted or monitored or decrypted information shall not be used or disclosed by the agency authorised under rule 4 for any other purpose, except for investigation or sharing with other security agency for the purpose of investigation or in judicial proceedings before the competent court in India.

(3) Save as otherwise provided in sub-rule (2), the contents of intercepted or monitored or decrypted information shall not be disclosed or reported in public by any means, without the prior order of the competent court in India. .

(4) Save as otherwise provided in sub-rule (2), strict confidentiality shall be maintained in respect of direction for interception, monitoring or decryption issued by concerned competent authority or the nodal officers.

(5) Any intermediary or its employees or person in-charge of computer resource who contravenes provisions of these rules shall be proceeded against and punished accordingly under, the relevant provisions of the Act for the time being in force.

(6) Whenever asked for by the concerned security agency at the Centre, the security agencies at the State and the Union territory level shall promptly share any information which they may have obtained following directions for interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource under rule 3, with the security agency at the Centre.