Rule 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 authorised 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

(iii) 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 of 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).