GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 1591
TO BE ANSWERED ON 04.12.2024

DIGITAL INDIA MISSION

†1591. SHRI ZIA UR REHMAN:

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

(a) the measures being taken by the Government to improve internet connectivity in rural and far flung areas under the Digital India Mission;
(b) whether the Government has taken any initiatives to stop the spread of fake news and misinformation;
(c) if so, the policy measures adopted in this regard and if not, the reasons therefor;
(d) whether the Government has taken any safety measures and implemented any schemes to control the cyber crimes and online fraud; and
(e) if so, the details thereof and if not, the reasons therefor?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a): The Government of India launched the National Broadband Mission on 17thDecember 2019, with a vision to enable fast-track growth of digital communications infrastructure and provide affordable and universal broadband access for all. The Mission aims to facilitate universal and equitable access to broadband services for growth and development throughout the country (especially in rural and remote areas).

The following actions were undertaken to enhance internet connectivity in rural and far flung areas.

(i) Centralized Right of Way portal: The GatiShakti Sanchar Portal (Centralized Portal for Right of Way Permissions) was launched on 14thMay 2022, to bring Ease of Doing Business for the applicants for quick Right of Way (RoW) permissions for laying OFC and erecting Telecom towers. The portal has on boarded/integrated all 36 States/UTs and four central ministries.
(ii) DoT has also come out with ITRoW (Indian Telegraph Right of Way) rules 2016, which were amended in Aug 2022 for the 5G roll-out. These rules provide for the standardization of rates for over ground and underground telecom infrastructure, rates for street furniture for utilization for 5G small cells, and charges applicable for compensation and restoration. DoT has followed up with all states/UTs to align their RoW policies with those of Central Right of Way rules and to clear pending Right of Way applications.

Further, the Telecommunication Act passed in 2023 and in accordance with this the Telecommunications (Right of Way) Rules, 2024 were brought in which will be in force from 1stJanuary 2025.

(b) to (e): The policies of Government of India are aimed at ensuring an open, safe, trusted and accountable cyberspace for users in the country. The key initiatives taken by Government of India to address challenges of fake news and misinformation in the cyberspace are as under:

The Ministry of Electronics and Information Technology ("Ministry") after extensive consultations with relevant stakeholders, has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021") in exercise of the powers given under the Information Technology Act, 2000 ("IT Act"). The IT Rules, 2021 cast specific due diligence obligations on intermediaries, including social media intermediaries, with respect to the information to make reasonable efforts by itself and to cause the user of their computer resource that is not to be hosted, displayed, uploaded, published, transmitted, stored or shared on the platforms. Intermediaries are required to ensure their accountability that includes their expeditious action towards removal of the unlawful information within the timelines prescribed under Rules. For this purpose, unlawful information comprises prohibited misinformation, patently false information, untrue or misleading in nature.

The IT Rules, 2021 also require the appointment of a Grievance Officer by intermediaries to resolve the complaints. Such Officer is required to provide time-bound redressal of the grievances of the victim / complainant against the violation of these rules. In case the victim / complainant is aggrieved by the decision of an intermediary's Grievance Officer or does not receive timely redressal, he/she may prefer an appeal to the Grievance Appellate Committee within thirty days of the receipt of communication from the Grievance Officer. In case of failure to observe due diligence as provided in the IT Rules, 2021, intermediaries lose the exemption from liability for any third-party information, data or communication link, under IT Act.

As an additional due diligence measure in IT Rules, 2021, the significant social media intermediaries ("SSMI")(i.e. a social media intermediary having 50 lakhs or above number of registered users in India)publish periodic compliance reports mentioning the information links that it has removed or disabled using automated tools. An SSMI, among other additional due diligences, is also required to cooperate with Law Enforcement Agencies (LEA) for prevention, detection, investigation, prosecution or punishment by enabling identification of the first originator of information related to the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, or public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material (CSAM).

Further, to address the emerging harms in the cyberspace like misinformation Ministry has conducted multiple consultations with industry stakeholders/ social media platforms and issued advisories through which the intermediaries were reminded about their due-diligence obligations outlined under theIT Rules, 2021and advised on countering unlawful content including malicious 'synthetic media' and 'deepfakes'. The government regularly engages with technology companies to sensitise them on the due diligence requirements under these Rules.

The Designated Officer appointed under the IT Act issues blocking orders to intermediaries for blocking access to specific information/ link (including the betting or gambling sites) in the interest of sovereignty and integrity, defence of India, security of the State, friendly relations with foreign States or public order or for inciting cognizable offence relating to above. MeitY follows due process as envisaged in the Information Technology (Procedure and Safeguards for Blocking for Access of Information for Public) Rules, 2009.

In addition to above, the Bharatiya Nyaya Sanhita, 2023 ("BNS") enacted in 2023 provides for stringent punishment against various crimes including cyber crimes. The BNS interalia defines "Organised crime" which includes economic offences, cyber-crimes, by any person or a group of persons, either as a member of an organised crime syndicate or on behalf of such syndicate. Several other provisions for punishment under the BNS may also be attracted in case of a cheating including cheating by personation, criminal breach of trust, forgery, etc. Most of these sections provide for non-bailable offences.

To spread awareness against cyber-crimes, the Government has been taking various initiatives from time to time. These, inter alia, includes cyber safety tips through social media, publishing of information security best practices, organizing cyber safety and security awareness programmes, etc.

MeitY launched a program titled Information Security Education & Awareness (ISEA) to generate awareness among users while using internet and to highlight the importance of internet related ethics advising them not to share rumours/fake news. A dedicated website has been created for information security awareness that generates and upgrades relevant awareness material on a regular basis, and can be accessed here https://www.infosecawareness.in.

The Indian Computer Emergency Response Team (CERT-In) has been taking various measures to prevent cyber frauds. These include issuance of alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on regular basis, conducting cyber security mock drills to assess the cyber security posture and preparedness of organisations.

RBI and banks have also been organising awareness campaigns through dissemination of short SMS, radio campaign, publicity on prevention of cybercrime etc. Further, RBI has been conducting electronic-banking awareness and training (e-BAAT) programmes about frauds and risk mitigation. Further, customers can also report financial frauds on the official customer care website or branches of the banks.

Further, to strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner, the Central Government has taken steps which, interalia, include-

(i) Establishment of the Indian Cyber Crime Coordination Centre (I4C);
(ii) Launching & operationalisation of 'National Cyber Crime Reporting Portal' (https://cybercrime.gov.in) and toll-free Helpline number '1930' to enable public to report cyber crimes, with special focus on cyber crimes against women and children;
(iii) Launching 'Citizen Financial Cyber Fraud Reporting and Management System' for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters;
(iv) Development of the Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. along with certification. More than 96,288 Police Officers from States/UTs are registered and more than 70,992 Certificates issued through the portal.

****