<div align="center">

GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
UNSTARRED QUESTION NO. 2426

</div>

TO BE ANSWERED ON THE 10TH DECEMBER, 2024/ AGRAHAYANA 19, 1946 (SAKA)

DIGITAL ARREST SCAM

2426.   SMT. KANIMOZHI KARUNANIDHI:

Will the Minister of HOME AFFAIRS be pleased to state:

(a) the total number of 'digital arrest scam' cases reported in the country, State/year-wise;

(b) the oversight mechanisms beyond CERT-In advisory guidelines to prosecute offenders in such cases; and

(c) the safeguards implemented by the Government to prevent digital arrest scams?

<div align="center">

ANSWER

</div>

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)

(a) to (c): 'Police' and 'Public Order' are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of crimes including cyber crime and digital arrest scams through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". The

latest published report is for the year 2022. Specific data regarding digital arrest scams is not maintained separately by NCRB.

To strengthen the mechanism to deal with cyber crimes including digital arrest scams in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

i. The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cybercrimes in the country, in a coordinated and comprehensive manner.

ii. The Central Government has launched a comprehensive awareness programme on digital arrest scams which, inter-alia, include; newspaper advertisement, announcement in Delhi Metros, use of social media influencers to create special posts, campaign through Prasar Bharti and electronic media, special programme on Aakashvani and participated in Raahgiri Function at Connaught Place, New Delhi on 27.11.2024.

iii. I4C proactively identify and blocked more than 1700 Skype IDs and 59,000 Whatsapp accounts used for Digital Arrest.

iv. The Central Government has published a Press Release on Alert against incidents of 'Blackmail' and 'Digital Arrest' by Cyber Criminals Impersonating State/UT Police, NCB, CBI, RBI and other Law Enforcement Agencies.

v.   The Central Government and Telecom Service Providers (TSPs) have devised a system to identify and block incoming international spoofed calls displaying Indian mobile numbers appear to be originating within India. Such international spoofed calls have been made by cyber-criminals in recent cases of fake digital arrests, FedEx scams, impersonation as government and police officials, etc. Directions have been issued to the TSPs for blocking of such incoming international spoofed calls.

vi.   Till 15.11.2024, more than 6.69 lakhs SIM cards and 1,32,000 IMEIs as reported by Police authorities have been blocked by Government of India.

vii. The 'National Cyber Crime Reporting Portal' (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.

viii. The 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the

fraudsters. So far, financial amount of more than Rs. 3431 Crore has been saved in more than 9.94 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.

ix.   To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, digital displays on railway stations and airports across, etc.

****