GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
STARRED QUESTION NO. *78
TO BE ANSWERED ON: 09.02.2024

CYBER SECURITY AND HACKING OF SOCIAL MEDIA

***78. SHRI K.R.N. RAJESHKUMAR:**

Will the Minister of Electronics and Information Technology be pleased to state:

(a) whether the Ministry discusses cyber security and hacking of social media accounts (like Facebook) of individual users with leading social media platforms;
(b) if so, whether social media platforms assured Government of its security features to prevent hacking;
(c) the number of hacking / digital impersonations of public persons complaints received by Government; and
(d) the security measures and commitments of social media platforms and Government's direction to the social media platforms to ensure cyber security of citizens.

ANSWER

MINISTER OF ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI ASHWINI VAISHNAW)

(a) to (d): A statement is laid on the Table of the House.

STATEMENT REFERRED TO IN THE REPLY TO RAJYA SABHA STARRED QUESTION NO. *78 FOR 09.02.2024 REGARDING CYBER SECURITY AND HACKING OF SOCIAL MEDIA

.....

(a) to (d): The policies of the Government are aimed at ensuring that internet in India is open, safe &trusted and accountable to all our users. Specifically, to deal with cyber security, Indian Computer Emergency Response Team ("CERT-In") is established under Section 70B of the Information Technology Act, 2000 ("IT Act"). CERT-In is the national nodal agency for responding to computer security incidents and has power to prescribe and implement reasonable security best practices. CERT-In may also call for information and give direction to the service providers, intermediaries (including social media intermediaries), data centres, body corporate and any other person for carrying out the provisions of functions under section 70B(4) of the IT Act.

CERT-In issued a direction on 28th April, 2022 mentioning types of cyber security incidents, including identity theft, spoofing and phishing attacks, to be mandatorily reported by service providers, intermediaries (including social media intermediaries), data centres, body corporate and Government organisations to CERT-In.

Additionally, CERT-In has also taken following measures to enhance awareness among organisations and users for safe usage of digital technologies and prevent cyber frauds:

a. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, mobile phones, networks and data on an ongoing basis. CERT-In has issued 72 advisories for organisations and users for data security, securing social media accounts and mitigating fraudulent activities.
b. On observing hacking of social media accounts, CERT-In coordinates incident response measures with affected entities and service providers.
c. CERT-In is working in coordination with service providers to track and disable phishing websites and facilitate investigation of fraudulent activities.
d. CERT-In has empanelled 177 security auditing organisations to support and audit implementation of Information Security Best Practices.
e. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and provides free tools to remove the same, and also provides cyber security tips and best practices for citizens and organisations.
f. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.
g. CERT-In is regularly carrying out various activities for development of cyber security capacities, skill building, awareness and citizen sensitization with respect to cyber-attacks and cyber frauds. In order to create security awareness within the Government, Public and Private Sector organizations, CERT-In regularly conducts trainings / workshops to train officials of Government, Public and Private sector organizations across all sectors and citizens on focused topics of Cyber Security. A total of 10074 officials from Government, critical sectors, public and private sector have been trained in 26 training programs in the area of cyber security during 2023.

CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Safer Internet Day on 7.2.2023 and Cyber Security Awareness Month in October 2023, by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with Centre for Development

of Advanced Computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices, etc., through videos and quizzes on the MyGov platform.

Rule 3(1)(b)(v) and (vi) of the IT Rules 2021 prohibits misinformation and patently false information on the Indian Internet or that impersonates another person. MeitY has, from time-to-time, issued advisories to the intermediaries for ensuring compliance with the prescribed due diligence and grievance reporting mechanism under the IT Rules, 2021.The failure to observe these rules will amount to non-compliance with the IT Rules, 2021 and result in the concerned intermediary automatically losing exemption from liability under section 79 of the IT Act. Government has also established Grievance Appellate Committees ("GAC") under the IT Rules, 2021 to allow users and victims to appeal online on www.gac.gov.in against decisions taken by the Grievance Officers of intermediaries.

As per information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), there were 6, 32 and 15 instances of hacking of social media accounts of users and organizations during the years 2021, 2022 and 2023 respectively. Further, 13,506 cases have been registered for cheating by personation by using computer resource (Section 66D IT Act) during year 2022.

Additionally, GAC has also received 205 appeals related of hacking/digital impersonation and 181 appeals have been disposed.

****

भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

राज्य सभा

तारांकित प्रश्न संख्या *78

जिसका उत्तर 09 फरवरी, 2024 को दिया जाना है।

20 माघ, 1945 (शक)

साइबर सुरक्षा और सोशल मीडिया की हैकिंग

***78. श्री के. आर. एन. राजेश कुमारः**

क्या इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री यह बताने की कृपा करेंगे कि:

(क) क्या मंत्रालय साइबर सुरक्षा और व्यक्तिगत उपयोगकर्ताओं के सोशल मीडिया खातों (जैसे फेसबुक) की हैकिंग के संबंध में प्रमुख सोशल मीडिया प्लेटफार्मों के साथ वार्ता करता है;

(ख) यदि हां, तो क्या सोशल मीडिया प्लेटफार्मों ने सरकार को हैकिंग को रोकने के लिए अपने सुरक्षा फीचर्स उपलब्ध कराने का आश्वासन दिया है;

(ग) सरकार को जनता की हैकिंग/प्रसिद्ध व्यक्तियों के डिजिटल प्रतिरूपण संबंधी कितनी शिकायतें प्राप्त हुई हैं; और

(घ) सोशल मीडिया प्लेटफार्मों के सुरक्षा उपाय और उनकी प्रतिबद्धताएं क्या हैं और नागरिकों की साइबर सुरक्षा सुनिश्चित करने के लिए सोशल मीडिया प्लेटफार्मों को सरकार ने क्या निर्देश दिए हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री (श्री अश्विनी वैष्णव)

(क) से **(घ)** : एक विवरण-पत्र सभा पटल पर रख दिया गया है।

*****

साइबर सुरक्षा और सोशल मीडिया की हैकिंग के संबंध में दिनांक 09.02.2024 को राज्य सभा में पूछे गए तारांकित प्रश्न सं. *78 के उत्तर में उल्लिखित विवरण-पत्र

*****

(क) से (घ): सरकार की नीतियों का उद्देश्य यह सुनिश्चित करना है कि भारत में इंटरनेट खुला, सुरक्षित और विश्वसनीय तथा हमारे सभी प्रयोक्ताओं के लिए जवाबदेह हो। विशेष रूप से, साइबर सुरक्षा से निपटने के लिए, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल ("सीईआरटी-इन") की स्थापना सूचना प्रौद्योगिकी अधिनियम, 2000 ("आईटी अधिनियम") की धारा 70 ख के तहत की गई है। सीईआरटी-इन कंप्यूटर सुरक्षा घटनाओं पर प्रतिक्रिया देने के लिए राष्ट्रीय नोडल एजेंसी है और इसके पास समुचित सुरक्षा श्रेष्ठ पद्धतियों को निर्धारित करने और लागू करने की शक्ति है। सीईआरटी-इन आईटी अधिनियम की धारा 70 ख(4) के तहत कार्यों के प्रावधानों को पूरा करने के लिए सेवा प्रदाताओं, मध्यस्थों (सोशल मीडिया मध्यस्थों सहित), डेटा केन्द्रों, निकाय निगमों और किसी अन्य व्यक्ति से जानकारी मांग सकता है और निदेश दे सकता है।

सीईआरटी-इन ने 28 अप्रैल, 2022 को एक निदेश जारी किया, जिसमें पहचान की चोरी, स्पूफिंग और फ़िशिंग हमलों सहित साइबर सुरक्षा घटनाओं के प्रकारों का उल्लेख किया गया, जिनकी रिपोर्ट सेवा प्रदाताओं, मध्यस्थों (सोशल मीडिया मध्यस्थों सहित), डेटा सेंटरों, निकाय निगमों और सरकारी संगठनों द्वारा सीईआरटी-इन को अनिवार्य रूप से दी जाएगी।

इसके अतिरिक्त, सीईआरटी-इन ने डिजिटल प्रौद्योगिकियों के सुरक्षित उपयोग और साइबर धोखाधड़ी को रोकने के लिए संगठनों और उपयोगकर्ताओं के बीच जागरूकता बढ़ाने के लिए निम्नलिखित उपाय भी किए हैं:

क. सीईआरटी-इन कम्प्यूटरों, मोबाइल फोनों, नेटवर्कों और डाटा की सुरक्षा के लिए अद्यतन साइबर खतरों/सुभेद्याताओं और प्रतिउपायों के संबंध में निरंतर आधार पर चेतावनियां और परामर्शी निदेश जारी करता है। सीईआरटी-इन ने संगठनों और उपयोगकर्ताओं के लिए डेटा सुरक्षा, सोशल मीडिया खातों को सुरक्षित करने और धोखाधड़ी युक्त गतिविधियों को कम करने के लिए 72 परामर्शी निदेश जारी किए हैं।

ख. सोशल मीडिया खातों की हैकिंग का पता चलने पर, सीईआरटी-इन प्रभावित संस्थाओं और सेवा प्रदाताओं के साथ घटना प्रतिक्रिया उपायों का समन्वय करता है।

ग. सीईआरटी-इन फिशिंग वेबसाइटों का पता लगाने और उन्हें अक्षम करने तथा धोखाधड़ी की गतिविधियों की जांच को सुकर बनाने के लिए सेवा प्रदाताओं के समन्वय से कार्य कर रहा है।

घ. सीईआरटी-इन ने सूचना सुरक्षा श्रेष्ठ पद्धतियों के कार्यान्वयन में सहायता और लेखापरीक्षण करने के लिए 177 सुरक्षा लेखापरीक्षा संगठनों को पैनलबद्ध किया है।

ङ. सीईआरटी-इन दुर्भावनापूर्ण प्रोग्रामों का पता लगाने के लिए साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) संचालित करता है और उन्हें हटाने के लिए मुफ्त उपकरण प्रदान करता है और नागरिकों और संगठनों के लिए साइबर सुरक्षा सुझाव और श्रेष्ठ पद्धतियाँ भी उपलब्ध कराता है।

च. सीईआरटी-इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक स्थितिजन्य जागरूकता पैदा करने के लिए राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) की स्थापना की है।

छ. सीईआरटी-इन साइबर सुरक्षा क्षमताओं के विकास, कौशल निर्माण, साइबर हमलों और साइबर धोखाधड़ियों के संबंध में नागरिकों को संवेदनशील बनाने के लिए नियमित रूप से विभिन्न कार्यकलाप कर रहा है। सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों में सुरक्षा जागरूकता पैदा करने के लिए सीईआरटी-इन नियमित रूप से साइबर सुरक्षा के केंद्रित विषयों पर सभी क्षेत्रों में सरकारी, सार्वजनिक और निजी क्षेत्र के संगठनों के अधिकारियों और नागरिकों को प्रशिक्षित करने के लिए प्रशिक्षण/कार्यशालाएं आयोजित करता है। वर्ष 2023 के दौरान साइबर सुरक्षा के क्षेत्र में 26 प्रशिक्षण कार्यक्रमों में सरकारी, महत्वपूर्ण क्षेत्रों, सार्वजनिक और निजी क्षेत्र के कुल 10074 अधिकारियों को प्रशिक्षित किया गया है।

सीईआरटी-इन नियमित रूप से अपने आधिकारिक सोशल मीडिया हैंडल और वेबसाइटों के माध्यम से साइबर सुरक्षा और संरक्षा पर सूचना का प्रसार करता है और सुरक्षा संबंधी सुझावों का आदान-प्रदान करता है। सीईआरटी-इन ने 7.2.2023 को सुरक्षित इंटरनेट दिवस और अक्टूबर 2023 में साइबर सुरक्षा जागरूकता माह के दौरान सोशल मीडिया प्लेटफॉर्म और वेबसाइटों पर पोस्टर और वीडियो का उपयोग करके सुरक्षा युक्तियाँ पोस्ट करके नागरिकों के लिए विभिन्न कार्यक्रमों और गतिविधियों का आयोजन किया। सीईआरटी-इन ने सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग के सहयोग से नागरिकों के लिए एक ऑनलाइन जागरूकता अभियान चलाया, जिसमें सामान्य ऑनलाइन सुरक्षा, सोशल मीडिया जोखिम और सुरक्षा, मोबाइल से संबंधित धोखाधड़ी और सुरक्षा, सुरक्षित डिजिटल भुगतान पद्धतियों आदि जैसे विषयों को शामिल किया गया।

आईटी नियमावली 2021 का नियम 3(1)(ख)(v) और (vi) भारतीय इंटरनेट पर गलत सूचना और स्पष्ट रूप से गलत जानकारी या किसी अन्य व्यक्ति का प्रतिरूपण करने पर रोक लगाता है। एमईआईटीवाई ने समय-समय पर आईटी नियमावली, 2021 के तहत निर्धारित अपेक्षित सावधानी और शिकायत रिपोर्टिंग तंत्र का अनुपालन सुनिश्चित करने के लिए मध्यस्थों को परामर्शी निदेश जारी किए हैं। इन नियमों का पालन करने में विफलता आईटी नियमावली, 2021 का गैर-अनुपालन माना जाएगा और इसके परिणामस्वरूप संबंधित मध्यस्थ स्वचालित रूप से आईटी अधिनियम की धारा 79 के तहत दायित्व से छूट खो देगा। सरकार ने आईटी नियमावली, 2021 के तहत शिकायत अपीलीय समितियों ("जीएसी") की भी स्थापना की है ताकि उपयोगकर्ताओं और पीड़ितों को मध्यस्थों के शिकायत अधिकारियों द्वारा लिए गए निर्णयों के विरुद्ध www.gac.gov.in पर ऑनलाइन अपील करने की सुविधा मिल सके।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) द्वारा ट्रैक की गई और इसको रिपोर्ट की गई जानकारी के अनुसार, वर्ष 2021, 2022 और 2023 के दौरान उपयोगकर्ताओं और संगठनों के सोशल मीडिया खातों की हैकिंग के क्रमशः 6, 32 और 15 मामले थे। इसके अलावा, वर्ष 2022 के दौरान कंप्यूटर संसाधन (आईटी अधिनियम की धारा 66घ) का उपयोग करके प्रतिरूपण द्वारा धोखाधड़ी के 13,506 मामले दर्ज किए गए हैं।

इसके अतिरिक्त, जीएसी को हैकिंग/डिजिटल प्रतिरूपण से संबंधित 205 अपीलें भी प्राप्त हुई हैं और 181 अपीलों का निपटान किया गया है।

****

SHRIMATI JAYA BACHCHAN: Sir, I would like to ask the Hon. Minister whether the Government has considered amending the Intermediary Rules under the IT Act. If so, the reasons thereof. And, whether the Government has any plans to introduce pre-censorship on online content and, if so, the details thereon.

SHRI ASHWINI VAISHNAW: Sir, Hon. Member has asked a very, very relevant and important question. I would like to answer this supplementary in three parts. First part is, yes, we are amending the Intermediary Rules. The reason for that is, the deepfake issue has come up in a very big way. Sir, today, social media platform and internet is an integral part of our lives. Practically everything that we do, whether it is banking, entertainment, reading news, etc., we are dependent on social media platforms and internet. With the spread of misinformation, deepfakes, we must take very strict and urgent action to make sure that this menace is removed. So, we are amending the Intermediary Rules. We are coming up with provisions where there is a significant responsibility bestowed on the social media platforms, so that they can detect deepfakes, misinformation and take early action. That is the first part. The second part is: Very clearly, the context of social media platforms and the safe harbor, which was there for many decades, has changed. Today, most of the social media platforms are already having their moderation technologies, moderation requirements and on the basis of that, they are already doing a lot of moderation. In that sense, platform is no longer a pure platform as it was, let us say, thirty years back. So, today, the entire world, the global regulatory community is reaching a kind of consensus and I also request the Hon. Members to develop some sort of consensus that the social media platforms will have to take more responsibility for what they are publishing on their platforms. That is the second part. The third part, Hon. Chairman, Sir, is: We are creating an institutional framework for the digital economy. That institutional framework has three parts — first is, having totally a new set of legislations. The Telecommunications Bill was passed by this esteemed House. The Digital Personal Data Protection Bill was passed by this esteemed House. There is another Bill in the working. The rules, regulations and the entire implementation mechanism are being converted into a total digital mechanism. We are also working very closely with almost every stakeholder to make sure that our internet is safe, trusted and delivering what it is supposed to do, Sir.

श्री राजीव शुक्ला: सभापति जी, मैं माननीय मंत्री जी से यह जानना चाहता हूँ कि आज साइबर क्राइम की स्थिति यह है कि इसका लोग इस कदर दुरुपयोग कर रहे हैं कि इसके माध्यम से वे लाखों लोगों का पैसा हड़प ले रहे हैं। तमाम राज्यों से इसको इस तरह के गैंग ऑपरेट करते हैं, जो

लोगों का पैसा हड़पते हैं। इस मामले में आप क्या-क्या कदम उठा रहे हैं, वह अपनी जगह है, लेकिन इसमें जहाँ तक सोशल मीडिया का जिक्र है, तो सोशल मीडिया एक ऐसा प्लेटफॉर्म हो गया है कि उस पर फ्रीडम ऑफ एक्सप्रेशन के नाम पर कोई भी व्यक्ति किसी के खिलाफ कुछ भी लिख सकता है। उसमें प्राइवेसी का कोई सवाल नहीं है, उसकी इज्जत का कोई सवाल नहीं है और वह कंटेंट उस पर सालों तक पड़ा रहता है। उसको आप हटवा नहीं सकते, क्योंकि जो प्लेटफॉर्म ओनर्स हैं, वे कहते हैं कि साहब, आप कोर्ट से ऑर्डर लीजिए।

MR. CHAIRMAN: Your supplementary, please.

श्री राजीव शुक्ला: कोर्ट से ऑर्डर लेने कौन जाए, कौन लेता है? जब कोई आदमी उसको खोलता है और देखता है कि अश्वनी वैष्णव के नाम से कुछ है, जिसमें 10 चीज़ें लिखी हुई हैं, तो वह समझता है कि यही असली अश्वनी वैष्णव हैं या यही राजीव शुक्ला हैं। असलियत यह है कि बात कुछ और होती है और लोग उन allegations के आधार पर अपना ओपिनियन फॉर्म करते हैं। आप इसको कैसे रोकेंगे? यह एक ऐसी प्रॉब्लम हो गई है कि इससे लोगों की प्राइवेसी छिन गई है। लोगों की जो अपनी इज्जत है, respect है, reputation है, उसके साथ खिलवाड़ हो रहा है। ...(**व्यवधान**)...

MR. CHAIRMAN: Now, Mr. Minister.

श्री राजीव शुक्ला: सर, ब्रॉडकास्टर्स के रेगुलेशंस हैं, न्यूज़पेपर्स के रेगुलेशंस हैं, लेकिन सोशल मीडिया में कोई accountability नहीं है। आप उसको कैसे फिक्स कर रहे हैं, उसका क्या प्रोविज़न ला रहे हैं? दूसरा यह कि ये कंटेंट वहां से कैसे हटें? तीसरा यह कि यू-ट्यूब चैनल वगैरह को जो आप ब्लॉक कर रहे हैं, वह एकतरफा नहीं होना चाहिए। इसके लिए कोई रूल बनना चाहिए। यह नहीं हो कि जो सरकार विरोधी है, उसको तो हटा दें और बाकी चलते रहें। इससे समस्या का हल नहीं निकलेगा। दूसरे लोग दुरुपयोग करेंगे। मेरा प्रश्न थोड़ा विस्तार से था, इसके लिए मैं क्षमा चाहता हूं। आशा है कि माननीय मंत्री जी जवाब देंगे।

MR. CHAIRMAN: Inspired by the Hon. Minister, the Hon. Member has asked his supplementary in three parts; and epicentre is Jaya Bachchan*ji*. *...(Interruptions)...*

SHRI ASHWINI VAISHNAW: I will answer in one part, Sir. सर, मैं इस प्रश्न का उत्तर एकदम संक्षेप में देना चाहूंगा। माननीय सदस्य ने एकदम सही बात कही है और जो प्वाइंट मैंने पिछले जवाब में कहा था कि सोशल मीडिया प्लेटफॉर्म्स को ज़िम्मेदारी लेनी चाहिए और इसके ऊपर इस हाउस में भी consensus बनना चाहिए, क्योंकि विश्व भर में आज एक consensus बन रहा है। सोशल मीडिया प्लेटफॉर्म के बारे में जैसा माननीय सदस्य ने कहा, मैं बताना चाहूंगा कि ऐसा नहीं हो सकता कि कोई भी, कुछ भी लिख दे और किसी की भी reputation के साथ खिलवाड़ कर दे। ऐसा नहीं होना चाहिए। समाज में सोशल मीडिया प्लेटफॉर्म की बहुत वैल्यू है,

उसकी पॉज़िटिव वैल्यू है और एक जो नेगेटिव इश्यू है, उसको सॉल्व करना भी हम सबकी ज़िम्मेदारी है। इसमें हाउस का एक consensus रहे कि जो भी गलत लिखता है, तो उसको तुरंत हटाने की पावर भी होनी चाहिए, मैथड भी होना चाहिए। सरकार ने एक institutional framework बनाया है, वह अब तक बहुत कारगर सिद्ध हुआ है और जैसे-जैसे हाउस में और consensus होगा, इसमें और कड़े कानून बनाने चाहिए।

MR. CHAIRMAN: Shrimati Priyanka Chaturvedi. ...*(Interruptions)*...

श्रीमती जया बच्चनः सर, मंत्री जी ने बहुत अच्छा जवाब दिया है, मगर ये जो भी मैथड यूज़ कर रहे हैं, वह कामयाब नहीं है। हमारे नाम से इंस्टाग्राम पर अकाउन्ट्स हैं। I am not on social media at all. मैं आपको बहुत पर्सनल चीज़ बता रही हूं। It is very nice of you to say 'consensus of the House', and everything. But, whatever methodology you are adopting is not working and it has become worse.

MR. CHAIRMAN: Thank you, Madam. I have made an exception.

श्रीमती प्रियंका चतुर्वेदीः सर, 30 अक्टूबर को मुझे एक एसएमएस आया था, काफी opposition MPs को ई-मेल आया था। ऐप्पल ने message भेजा था, 'State-sponsored attackers may be attacking your i-phone'. उसके संदर्भ में उसी दिन मैंने माननीय आईटी मिनिस्टर को चिट्ठी लिखी थी, आज 4 महीने होने वाले हैं, उसका कोई जवाब नहीं आया है। सर, उन्होंने एक बहुत constructive suggestion दिया कि एक orientation course होना चाहिए, ऐसे ही orientation course मिनिस्टर्स के लिए भी होने चाहिए कि time bound चिट्ठी का जवाब दें।

दूसरा यह कि राज्य सभा की एक मेम्बर ऑफ पार्लियामेंट के ऊपर लोक सभा में नाम लेकर allegation न लगाएं, यह आपके संज्ञान में भी है।

MR. CHAIRMAN: I will answer for the first one. If any Hon. Member feels that an Hon. Minister is not responding to the communications of the Hon. Member, approach your Chairman. ...*(Interruptions)*... Please take your seat. ...*(Interruptions)*... Take your seat.

श्री अश्वनी वैष्णवः सर, अगर किसी को लगता है कि उसके फोन में कोई प्रॉब्लम है - सर, हमारे यहां एक बहुत अच्छा institutional mechanism है, CERT-In is a highly qualified technical organization. It is purely a technical organization. आप अपना फोन दीजिए। सर, हमने openly कहा है, I have said that in public through a press conference that if any Hon. Member or any honourable citizen of the country has any issue related to hacking of their phone or something, kindly share that information, kindly share the details, kindly submit your phone, we will get it technically examined. ...*(Interruptions)*...

MR. CHAIRMAN: Just one minute. ...*(Interruptions)*... Priyanka*ji*, you are a senior person. Please don't do it and take your seat.

श्री अश्वनी वैष्णवः सर, ऐसा नहीं हो सकता कि केवल allegation लगाएं। अगर कोई allegation लगाता है, तो साथ में जो law enforcement की एजेंसीज़ हैं, जो स्ट्रक्चर है, सिस्टम है, उस सिस्टम के साथ आपको co-operate भी करना पड़ेगा। वन वे नहीं चलता है...(**व्यवधान**)... वन वे नहीं चलता है।...(**व्यवधान**)... आप अगर बार-बार कहते हैं, एक माननीय सदस्य कहते हैं कि social media ...*(Interruptions)*..

MR. CHAIRMAN: No. ...*(Interruptions)*.. Hear the Hon. Minister. ...*(Interruptions)*.. Shrimati Priyanka Chaturvedi, please; first hear the Minister. ...*(Interruptions)*.. Hear the Minister. ...*(Interruptions)*.. No; please hear the Minister. ...*(Interruptions)*.. Can I allow it? You asked a question. The Minister did not get up because he was not allowed to get up. ..*(Interruptions)*...

SHRIMATI PRIYANKA CHATURVEDI: Why don't you allow, Sir?

MR. CHAIRMAN: I must have some sanction imposed and one sanction is, please ask question when I say so. Now, Hon. Minister.

श्री अश्वनी वैष्णवः अगर कोई आरोप लगाता है कि भारत सरकार...(**व्यवधान**)... माननीय सदस्य ने आरोप लगाया है, तो इनकी जिम्मेदारी बनती है as a citizen of this country and as a Member of this House to absolutely cooperate in the investigation, so that the truth would come out. This is what I have been requesting. I have done that through a Press Conference. I have done in this House itself when the Post Office Bill was being discussed. If the Hon. Member just stands there to make allegation, that is not the way a Member should be behaving.

MR.CHAIRMAN: Now, Question No. 79. ..*(Interruptions)*.. Shrimati Geeta alias Chandraprabha. ..*(Interruptions)*.. Nothing will go on record. Dr. John Brittas, ...(*Interruptions*).. No, Madam Jaya Bachchan. ...(*Interruptions*).. Question No. 79, Shrimati Geeta alias Chandraprabha. ...*(Interruptions)*.. Hon. Minister, Question No. 79. ...*(Interruptions)*.. Yes, Madam. ...*(Interruptions)*.. First supplementary, please.