

भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 4342
जिसका उत्तर 26 मार्च, 2025 को दिया जाना है।
05 चैत्र, 1947 (शक)

साइबर सुरक्षा कानूनों का सुदृढीकरण

4342. श्रीमती लवली आनंद:

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

- (क) सरकार द्वारा साइबर अपराधों को रोकने के लिए क्या उपाय किए जा रहे हैं;
- (ख) डिजिटल इंडिया अभियान के तहत अब तक राज्यवार कितने गांवों को इंटरनेट सुविधा प्रदान की गई है; और
- (ग) सरकार द्वारा साइबर सुरक्षा कानूनों को सुदृढ बनाने के लिए क्या कदम उठाए गए हैं?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क)से (ग): सरकार की नीतियों का उद्देश्य अपने प्रयोक्ताओं के लिए एक खुला, सुरक्षित, विश्वसनीय और जवाबदेह इंटरनेट सुनिश्चित करना है। इस लक्ष्य को प्राप्त करने में सहायता करने और साइबर सुरक्षा अवसंरचना और कानूनों को व्यापक और समन्वित तरीके से सुदृढ करने के लिए किए गए प्रयासों सहित साइबर अपराधों से निपटने के लिए तंत्र को सुदृढ करने के लिए केन्द्र सरकार ने अनेक कदम उठाए हैं जो निम्नानुसार हैं:

- i. भारत सरकार (कार्याबंटन) नियमावली, 1961 (एओबीआर) में इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) को साइबर कानूनों, सूचना प्रौद्योगिकी अधिनियम, 2000 (आईटी अधिनियम) और आईटी से संबंधित अन्य कानूनों के प्रशासन से संबंधित मामले आबंटित किए गए हैं। इसके अलावा, देश की साइबर सुरक्षा स्थिति को सुव्यवस्थित करने के लिए 27.09.2024 को एओबीआर में संशोधन किया गया है। इस संशोधन के माध्यम से, दूरसंचार नेटवर्कों की सुरक्षा से संबंधित मामले दूरसंचार विभाग (डीओटी) को आबंटित किए गए हैं, सूचना प्रौद्योगिकी अधिनियम के अंतर्गत आने वाले साइबर सुरक्षा से संबंधित मामले और साइबर सुरक्षा पर अन्य मंत्रालयों/विभागों को समर्थन इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) को आबंटित किया गया है, साइबर अपराध से संबंधित मामले गृह मंत्रालय (एमएचए) को आबंटित किए गए हैं तथा साइबर सुरक्षा के लिए समग्र समन्वय और रणनीतिक निदेशों का दायित्व राष्ट्रीय सुरक्षा परिषद सचिवालय को आबंटित किया गया है।
- ii. भारत और भारतीय इंटरनेट के उपयोगकर्ताओं को प्रौद्योगिकियों के दुरुपयोग से उत्पन्न होने वाले उभरते नुकसान, आपराधिकता और ऐसे अन्य संबंधित जोखिमों से बचाने और देश के कानून के प्रति जवाबदेही सुनिश्चित करने के लिए, एमईआईटीवाई लगातार जनता और हितधारकों के साथ जुड़ता है और उनसे इनपुट प्राप्त करता है, जिसमें नए कानूनों का निर्माण, मौजूदा कानूनों को मजबूत करना और लागू करना और अनुपालन के स्तर की निगरानी करना शामिल है। इस संबंध में, सूचना प्रौद्योगिकी अधिनियम वर्ष 2000 में अधिसूचित किया गया था और साइबर स्पेस में प्रयोक्ताओं की सुरक्षा के लिए समय-समय पर इसमें संशोधन किया जा रहा

है। इसके अलावा, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 (डीपीडीपी अधिनियम) अधिनियमित किया गया है जो डेटा सुरक्षा के लिये रूपरेखा प्रदान करता है।

- iii. सूचना प्रौद्योगिकी अधिनियम में अनेक अपराधों को परिभाषित किया गया है और इसमें विभिन्न साइबर अपराधों और डाटा उल्लंघनों जैसे कम्प्यूटर, कम्प्यूटर प्रणाली आदि को क्षति पहुंचाने के लिए दंड और क्षतिपूत, डाटा की सुरक्षा करने में विफलता के लिए मुआवजा, कम्प्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़ करने के लिए सजा, कम्प्यूटर से संबंधित अपराधों के लिए सजा, पहचान की चोरी के लिए सजा, कम्प्यूटर संसाधन का उपयोग करके प्रतिरूपण द्वारा धोखाधड़ी के लिए दंड, साइबर आतंकवाद और संरक्षित प्रणाली तक अप्राधिकृत पहुँच हासिल करने इत्यादि के लिए दंड का प्रावधान है।
- iv. भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) को आईटी अधिनियम के तहत नोडल एजेंसी के रूप में स्थापित किया गया है, जो साइबर सुरक्षा के क्षेत्र में कार्य करता है जैसे साइबर घटनाओं पर सूचना का संग्रह, विश्लेषण और प्रसार, साइबर सुरक्षा घटनाओं का पूर्वानुमान और अलर्ट, साइबर सुरक्षा घटनाओं से निपटने के लिए आपातकालीन उपाय, साइबर घटना प्रतिक्रिया गतिविधियों का समन्वय, सूचना सुरक्षा प्रथाओं, प्रक्रियाओं, रोकथाम, प्रतिक्रिया और घटना प्रतिक्रिया के लिए साइबर घटनाओं की रिपोर्टिंग से संबंधित दिशानिर्देश, सलाह, भेद्यता नोट और श्वेत पत्र जारी करना।
- v. इसके अतिरिक्त, सीईआरटी-इन साइबर स्वच्छता केंद्र (सीएसके) का संचालन करता है, जो स्वच्छ भारत के दृष्टिकोण को साइबर स्पेस तक विस्तारित करने के लिए एक नागरिक-केंद्रित पहल है, जो बोटनेट सफाई और मेलवेयर विश्लेषण सेवाएं प्रदान करता है। सीएसके दुर्भावनापूर्ण कार्यक्रमों का पता लगाने में मदद करता है, मुफ्त निष्कासन उपकरण प्रदान करता है, और उपयोगकर्ताओं को सर्वोत्तम साइबर सुरक्षा पद्धतियों के विषय पर शिक्षित करता है। इसके अलावा, सीईआरटी-इन एक स्वचालित साइबर थ्रेट इंटेलिजेंस एक्सचेंज प्लेटफॉर्म का संचालन करता है जो सक्रिय रूप से सभी क्षेत्रों में संगठनों के साथ साइबर खतरे के अलर्ट को एकत्र, विश्लेषण और साझा करता है, जिससे उन्हें उभरते खतरों के खिलाफ निवारक उपाय करने में सक्षम बनाया जा सके।
- vi. राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना आईटी अधिनियम के तहत महत्वपूर्ण सूचना अवसंरचना संरक्षण के संबंध में राष्ट्रीय नोडल एजेंसी के रूप में की गई है। एनसीआईआईपीसी महत्वपूर्ण सूचना अवसंरचना की सुरक्षा से संबंधित अनुसंधान और विकास सहित सभी उपायों के लिए जिम्मेदार है।
- vii. व्यक्तिगत डेटा की सुरक्षा के संबंध में, सूचना प्रौद्योगिकी (उचित सुरक्षा पद्धतियाँ और प्रक्रियाएं और संवेदनशील व्यक्तिगत डेटा या सूचना) नियम, 2011 को संवेदनशील व्यक्तिगत डेटा या सूचना पर उचित सुरक्षा प्रथाओं और प्रक्रियाओं को निर्धारित करते हुए अधिसूचित किया गया है। इसके अलावा, डी पी डी पी अधिनियम डिजिटल व्यक्तिगत डेटा को संसाधित करते समय सुरक्षा संरक्षोपायों के साथ-साथ मजबूत तकनीकी और संगठनात्मक उपायों को लागू करने के लिए डेटा फिड्यूशरीज़ को अधिदेशित करता है। यह किसी भी व्यक्तिगत डेटा उल्लंघन या कानून के अन्य उल्लंघनों के लिए डेटा फिड्यूशरीज़ को जवाबदेह ठहराता है। डेटा संरक्षण बोर्ड उल्लंघनों का निर्णय करके और गैर-अनुपालन के लिए वित्तीय दंड लगाकर इस जवाबदेही को सुनिश्चित करता है।

- viii. इसके अलावा, डीओटी ने साइबर हमलों से निपटने और दूरसंचार बुनियादी ढांचे की साइबर सुरक्षा सुनिश्चित करने के उपायों का प्रावधान करने के लिए दूरसंचार अधिनियम, 2023 के तहत दूरसंचार (दूरसंचार साइबर सुरक्षा) नियम, 2024 और दूरसंचार (महत्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024 को अधिसूचित किया है।
- ix. डीओटी ने मोबाइल ग्राहकों को सशक्त बनाने, उनकी सुरक्षा को मजबूत करने और सरकार की नागरिक केंद्रित पहलों के बारे में जागरूकता बढ़ाने के लिए नागरिक-केंद्रित पहल के रूप में संचार साथी पोर्टल लॉन्च किया है। यह पोर्टल संदिग्ध धोखाधड़ी संचार की रिपोर्टिंग, चोरी या खोए हुए मोबाइल हैंडसेट को अवरुद्ध करने और ट्रेस करने का अनुरोध करने, मोबाइल हैंडसेट की वास्तविकता की जांच करने और अंतरराष्ट्रीय कॉल की रिपोर्ट करने की सुविधा प्रदान करता है जो कॉलिंग लाइन पहचान के रूप में एक भारतीय टेलीफोन नंबर को गलत तरीके से प्रदर्शित करता है।
- x. दूरसंचार विभाग ने फर्जी या जाली दस्तावेजों का उपयोग करके प्राप्त धोखाधड़ी वाले मोबाइल कनेक्शनों का पता लगाने के लिए एक प्रणाली विकसित की है। इसके अतिरिक्त, साइबर अपराधों और वित्तीय धोखाधड़ी को रोकने के लिए हितधारकों के साथ दूरसंचार संसाधनों और डिस्कनेक्ट किए गए नंबरों के दुरुपयोग से संबंधित जानकारी साझा करने की सुविधा उपलब्ध कराने के लिए एक ऑनलाइन डिजिटल इंटेलिजेंस प्लेटफॉर्म (डीआईपी) लॉन्च किया गया है। भारतीय मोबाइल नंबरों को गलत तरीके से प्रदर्शित करने वाली अंतरराष्ट्रीय नकली कॉल पर अंकुश लगाने के लिए, दूरसंचार विभाग और टीएसपी ने ऐसी कॉल की पहचान करने और उन्हें ब्लॉक करने के लिए एक प्रणाली तैयार की है, जिनका अक्सर साइबर अपराधियों द्वारा धोखाधड़ी और प्रतिरूपण के लिए दुरुपयोग किया जाता है।
- xi. गृह मंत्रालय ने देश में सभी प्रकार के साइबर अपराधों से निपटने के लिए एक संबद्ध कार्यालय के रूप में 'भारतीय साइबर अपराध समन्वय केंद्र' (I4C) की स्थापना की है। I4C के हिस्से के रूप में, एन सी आर पी (<https://cybercrime.gov.in>) को जनता को साइबर अपराध की घटनाओं की रिपोर्ट करने में सक्षम बनाने के लिए लॉन्च किया गया है। चूंकि भारत के संविधान की सातवीं अनुसूची के अनुसार 'पुलिस' और 'लोक व्यवस्था' राज्य के विषय हैं, इसलिए राज्य/संघ राज्य क्षेत्र साइबर अपराध सहित अपराधों की रोकथाम करने, पता लगाने, जांच और अभियोजन के लिए अपनी विधि प्रवर्तन एजेंसियों (एलईए) के माध्यम से प्राथमिक रूप से उत्तरदायी हैं।
- xii. साइबर अपराध की जांच, फॉरेंसिक, अभियोजन आदि के महत्वपूर्ण पहलुओं पर ऑनलाइन पाठ्यक्रम के माध्यम से पुलिस अधिकारियों/न्यायिक अधिकारियों की क्षमता निर्माण के लिए मैसिव ओपन ऑनलाइन कोर्सेज (एमओओसी) प्लेटफॉर्म, जिसका नाम 'साइट्रेन' पोर्टल है, को आई4सी के तहत विकसित किया गया है। इसके अलावा, I4C ने बैंकों और वित्तीय संस्थानों के सहयोग से साइबर अपराधियों की एक संदिग्ध रजिस्ट्री शुरू की है, जो साइबर धोखाधड़ी को ट्रैक करने और रोकने के प्रयासों को मजबूत करती है।
- xiii. मोबाइल इंटरनेट कवरेज वाले गांवों की संख्या के संबंध में राज्य-वार आंकड़े **अनुबंध- I में दिए गए हैं।**

31-12-2024 तक की स्थिति के अनुसार राज्य/संघ राज्य क्षेत्र वार गांवों में मोबाइल इंटरनेट कवरेज स्थिति

क्र. सं.	राज्य/संघ राज्य क्षेत्र	सूचीबद्ध 6,44,131 गांवों में से मोबाइल इंटरनेट युक्त गाँव
1.	अंडमान और निकोबार द्वीप समूह	389
2.	आंध्र प्रदेश	16285
3.	अरुणाचल प्रदेश	4141
4.	असम	25969
5.	बिहार	44781
6.	चंडीगढ़	0
7.	छत्तीसगढ़	19123
8.	दादरा और नगर हवेली और दमन और दीव	95
9.	गोवा	344
10.	गुजरात	17932
11.	हरियाणा	6640
12.	हिमाचल प्रदेश	20112
13.	जम्मू और कश्मीर	6062
14.	झारखंड	31725
15.	कर्नाटक	29134
16.	केरल	1438
17.	लद्दाख	225
18.	लक्षद्वीप	23
19.	मध्य प्रदेश	53899
20.	महाराष्ट्र	41570
21.	मणिपुर	2211
22.	मेघालय	6324
23.	मिजोरम	740
24.	नागालैंड	1202
25.	राष्ट्रीय राजधानी क्षेत्र दिल्ली	55
26.	ओडिशा	48573
27.	पुडुचेरी	96
28.	पंजाब	12532
29.	राजस्थान	44389
30.	सिक्किम	441
31.	तमिलनाडु	16424
32.	तेलंगाना	9964
33.	त्रिपुरा	702
34.	उत्तर प्रदेश	105461
35.	उत्तराखंड	15901
36.	पश्चिम बंगाल	40951
कुल		625853