भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 2389

जिसका उत्तर 21 दिसम्बर, 2022 को दिया जाना है।

30 अग्रहायण, 1944 (शक)

व्यक्तिगत और निजी डेटा लीकेज

2389. श्री सुनील दत्तात्रेय तटकरे :

श्रीमती सुप्रिया सदानंद सुले :

डॉ. सुभाष रामराव भामरे :

डॉ. अमोल रामसिंह कोल्हे :

श्री कुलदीप राय शर्मा :

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

(क) वर्ष 2015 से लोगों की सहमति के बिना सोशल मीडिया कंपनियों, निजी संस्थाओं, सरकार या किसी अन्य संगठन, संस्था या निकाय द्वारा भारतीयों के व्यक्तिगत और निजी डेटा को कथित रूप से लीक या साझा किए जाने के कुल मामलों की संख्या कितनी है;

(ख) संबंधित अधिकारियों द्वारा प्रत्येक व्यक्तिगत मामले में की-गई-कार्रवाई और लोगों को प्रदान किए गए समाधान, यदि कोई हो, क्या है;

(ग) क्या सरकार द्वारा इन मामलों के पीड़ितों को कोई मुआवजा दिया गया था और यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(घ) क्या सरकार का कंपनियों को उपयोगकर्ता डेटा की सुरक्षा के लिए कदम उठाने का कोई निर्देश है और यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं;

(ड.) क्या सरकार सहमति मांगे बिना किसी भी तरह के लोगों की व्यक्तिगत जानकारी एकत्र, उपयोग और साझा कर सकती है; और

(च) यदि हां, तो कानूनी रूप से सरकार किस सीमा तक लोगों की स्पष्ट सहमति के बिना किसी भी तरह से उनकी व्यक्तिगत जानकारी एकत्र करने, साझा करने और उपयोग करने के लिए स्वतंत्र है ?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क): साइबर स्पेस अज्ञात और सीमा रहित है और तकनीकी नवाचारों और विभिन्न प्रकार के उपकरणों और सेवाओं को शामिल करने के साथ बहुत ही परिष्कृत और जटिल हो गया है। भारतीय उपयोगकर्ताओं के किसी भी डेटा उल्लंघन की सूचना भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (सीईआरटी-इन) को दी जानी चाहिए, जो देश में घटना की प्रतिक्रिया के लिए और साइबर घटनाओं पर जानकारी एकत्र करने के लिए राष्ट्रीय नोडल एजेंसी है। सीईआरटी-इन को दी गई और इसके द्वारा

ट्रैक की गई जानकारी के अनुसार, वर्ष 2020, 2021 और 2022 (नवंबर तक) के दौरान क्रमशः कुल 14, 6 और 22 घटनाएं दर्ज की गईं ।

(ख): डेटा रिसाव या उल्लंघन को देखने पर, सीईआरटी-इन ने किए जाने वाले उपचारात्मक कार्यों के साथ प्रभावित संगठनों को अधिसूचित किया। सीईआरटी-इन घटना प्रतिक्रिया उपायों में प्रभावित संगठनों, सेवा प्रदाताओं और संबंधित क्षेत्र के नियामकों के साथ भी समन्वित किया । इसके अलावा, लोगों और संगठनों को शिक्षित करने के लिए, सीईआरटी-इन ने नवीनतम साइबर-खतरों/भेद्यताओं और प्रतिउपायों के बारे में निरंतर आधार पर अलर्ट और सलाह भी जारी की है।

(ग) और (घ): सूचना प्रौद्योगिकी अधिनियम, 2000 ("आईटी अधिनियम") धारा 43ए में प्रावधान है कि एक निकाय कॉर्पोरेट जिसके पास एक कंप्यूटर संसाधन में कोई संवेदनशील व्यक्तिगत डेटा या जानकारी है, जिसका वह मालिक है, नियंत्रण या संचालन करता है उचित सुरक्षा प्रथाओं और प्रक्रियाओं को लागू करने और बनाए रखने में लापरवाही के कारण किसी भी व्यक्ति को गलत नुकसान या गलत लाभ के कारण प्रभावित व्यक्ति को मुआवजे के रूप में नुकसान का भुगतान करने के लिए उत्तरदायी है। सरकार ने उक्त धारा के तहत अपनी शक्तियों का प्रयोग करते हुए, सूचना प्रौद्योगिकी (उचित सुरक्षा प्रथाओं और प्रक्रियाओं और संवेदनशील व्यक्तिगत डेटा या सूचना) नियम, 2011 (एसपीडीआई नियम) बनाए हैं, सुरक्षा प्रथाओं और प्रक्रियाओं को निर्धारित करते हुए कि एक निकाय कॉर्पोरेट या ऐसे निकाय कॉर्पोरेट की ओर से जानकारी एकत्र करने, प्राप्त करने, रखने, भंडारण करने, व्यवहार करने या संभालने वाले किसी भी व्यक्ति को उपयोगकर्ताओं के व्यक्तिगत डेटा की सुरक्षा के लिए निगरानी रखना आवश्यक है। इनमें ऐसी आवश्यकताएं शामिल हैं जो ऐसे निकाय कॉर्पोरेट या व्यक्ति वेबसाइट पर गोपनीयता और व्यक्तिगत जानकारी, डेटा या जानकारी के प्रकटीकरण के लिए एक नीति प्रकाशित करते हैं, एकत्र की गई जानकारी का उपयोग उस उद्देश्य के लिए करते हैं जिसके लिए इसे एकत्र किया गया था, इसे सुरक्षित रखें, और संवेदनशील व्यक्तिगत डेटा प्रकट करने के लिए सूचना प्रदाता से पूर्व अनुमति प्राप्त करें। । इन नियमों के उल्लंघन पर पीड़ित व्यक्ति आईटी अधिनियम के तहत न्यायनिर्णायक अधिकारी से मुआवजे के लिए संपर्क कर सकता है। सरकार ने इस उद्देश्य के लिए प्रत्येक राज्य और केंद्र शासित प्रदेश के सूचना प्रौद्योगिकी विभाग के सचिव को न्यायनिर्णायक अधिकारी नियुक्त किया है। सरकार पीड़ितों को दिए गए मुआवजे का रिकॉर्ड नहीं रखती है।

इसके अलावा , आईटी अधिनियम की धारा 72क वैध अनुबंध के उल्लंघन में सूचना के प्रकटीकरण के लिए सजा का प्रावधान करती है।

गृह मंत्रालय के तहत भारतीय साइबर अपराध समन्वय केंद्र (I4ग) को साइबर अपराध के खिलाफ लड़ाई में नोडल बिंदु के रूप में नामित किया गया है। नागरिकों को अपनी भाषा में ऑनलाइन शिकायत दर्ज करने में सहायता प्राप्त करने के लिए एक टोल-फ्री नंबर 1930 चालू किया गया है। साइबर अपराध पर जागरूकता फैलाने के लिए, गृह मंत्रालय ने कई कदम उठाए हैं जिनमें ट्विटर हैंडल @ cyberDost और रेडियो अभियानों के माध्यम से साइबर अपराध पर संदेशों का प्रसार शामिल है।

उपरोक्त के अलावा, साइबर सुरक्षा स्थिति को बढ़ाने और डेटा लीक को रोकने के लिए निम्नलिखित उपाय किए गए हैं:

(i) सीईआरटी -नवीनतम लिए के सुरक्षा की नेटवर्क और कंप्यूटर पर आधार निरंतर इन-साइबर खतरोहै। करता जारी सलाह और अलर्ट में बारे के प्रतिउपायों /और भेद्यताओं/

(ii) उपयोगकर्ताओं को अपने डेस्कटॉप और मोबाइल फोन को सुरक्षित रखने और फ़िशिंग हमलों को रोकने के लिए सुरक्षा युक्तियाँ प्रकाशित की गई हैं।

(iii) सीईआरटी-इन ने केंद्र सरकार के सभी मंत्रालयों और विभागों, राज्य सरकारों और उनके संगठनों और महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए साइबर हमलों और साइबर आतंकवाद का मुकाबला करने के लिए एक साइबर संकट प्रबंधन योजना तैयार की है।

(iv) सीईआरटी-इन नेटवर्क और सिस्टम प्रशासकों और सरकार और महत्वपूर्ण क्षेत्र के संगठनों के मुख्य सूचना सुरक्षा अधिकारियों के लिए सूचना प्रौद्योगिकी के बुनियादी ढांचे को सुरक्षित करने और साइबर हमलों को कम करने के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है।

(v) सभी सरकारी वेबसाइटों और एप्लिकेशन को उन्हें होस्ट करने से पहले साइबर सुरक्षा के संबंध में ऑडिट किया जाता है। होस्टिंग के बाद भी वेबसाइटों और एप्लिकेशन का ऑडिट नियमित आधार पर किया जाता है।

(vi) सीईआरटी-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और ऑडिट करने के लिए 150 सुरक्षा ऑडिटिंग संगठनों को सूचीबद्ध किया है।

(vii) सीईआरटी-इन छोटे छोटे अलर्ट को सक्रिय रूप से एकत्र करने, विश्लेषण करने और विभिन्न क्षेत्रों के संगठनों के साथ उनके द्वारा सक्रिय खतरे को कम करने के लिए उनके अनुरूप साझा करने हेतु एक स्वचालित साइबर-खतरा विनिमय मंच संचालित करता है।

(viii) सरकार और महत्त्वपूर्ण क्षेत्रों में संगठनों की साइबर सुरक्षा मुद्रा और तैयारी के आकलन को सक्षम करने के लिए साइबर सुरक्षा मॉक ड्रिल आयोजित की जा रही है ।

(ix) सीईआरटी-इन दुर्भावनापूर्ण प्रोग्रामों का पता लगाने और उन्हें हटाने के लिए मुफ़्त टूल और नागरिकों और संगठनों के लिए साइबर सुरक्षा टिप्स और सर्वोत्तम अभ्यास प्रदान करने के लिए साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) का संचालन करता है।

(x) सीईआरटी-इन अपने आधिकारिक सोशल मीडिया हैंडल और वेबसाइटों के माध्यम से नियमित रूप से सूचना का प्रसार करता है और साइबर सुरक्षा पर सुरक्षा युक्तियों को साझा करता है।

(xi) इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय सूचना सुरक्षा जागरूकता उत्पन्न करने के लिए कार्यक्रम आयोजित करता है। सूचना सुरक्षा के बारे में बच्चों, माता-पिता और सामान्य उपयोगकर्ताओं के लिए विशिष्ट पुस्तकें, वीडियो और ऑनलाइन सामग्री विकसित की जाती हैं, जिन्हें www.infosecawareness.in और www.csk.gov.in जैसे पोर्टलों के माध्यम से प्रसारित किया जाता है ।

(ङ) और (च): नहीं महोदय /महोदया । सरकार सहित किसी व्यक्ति द्वारा व्यक्तिगत जानकारी के संग्रह, उपयोग और साझा करने के संबंध में कानूनी आवश्यकता, वर्तमान में लागू विभिन्न कानूनों और किसी भी प्रासंगिक बाध्यकारी न्यायिक निर्णयों से उत्पन्न होती है।

एस्पीडीआई नियम, 2011 के अनुसार एक निकाय कॉर्पोरेट के लिए यह आवश्यक है कि संवेदनशील व्यक्तिगत डेटा का खुलासा करने के लिए सूचना प्रदाता की पूर्व अनुमति प्राप्त किया जाए , जब तक कि इस तरह के प्रकटीकरण पर निकाय कॉर्पोरेट और सूचना प्रदाता के बीच अनुबंध पर सहमति न हो, या कानूनी बाध्यता के अनुपालन के लिए यह आवश्यक हो या पहचान या रोकथाम, पहचान, जांच, अभियोजन और अपराधों की सजा के सत्यापन के उद्देश्य से जानकारी प्राप्त करने के लिए कानून के तहत अनिवार्य सरकारी एजेंसियों के साथ जानकारी साझा न की जानी हो ।

इसके अलावा, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय ने डिजिटल व्यक्तिगत डेटा संरक्षण विधेयक, 2022 शीर्षक से एक मसौदा विधेयक तैयार किया है और अपने सार्वजनिक परामर्श अभ्यास के हिस्से के रूप में जनता से प्रतिक्रिया आमंत्रित की है। ड्राफ्ट बिल नागरिक (डिजिटल नागरिक) के अधिकारों और कर्तव्यों को निर्धारित करता है और कानूनी रूप से एकत्रित डेटा का उपयोग करने के लिए डेटा न्यासी के दायित्वों को निर्धारित करता है।

****

*****