भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
राज्य सभा
अतारांकित प्रश्न संख्या 2007
जिसका उत्तर **17 मार्च, 2023** को दिया जाना है ।
26 फाल्गुन, 1944 (शक)

आधार डेटाबेस का लीक होना

2007. श्रीमती वंदना चव्हाण :

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

(क) क्या सरकार हाल ही के ऐसे सुरक्षा उल्लंघनों से अवगत है जहां आधार को लीक करके नागरिकों के अन्य व्यक्तिगत डेटा के साथ बेचा जा रहा है;
(ख) पिछले पांच वर्षों में आधार डाटाबेस के लीक होने के कितने मामले दर्ज किए गए हैं;
(ग) आधार डेटाबेस तक ऐसी अनधिकृत पहुंच से जुड़े विभिन्न खतरे क्या हैं; और
(घ) साइबर सुरक्षा को मजबूत बनाने और सुरक्षा के ऐसे उल्लंघनों को रोकने के लिए सरकार द्वारा क्या कदम उठाए गए हैं ?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क) : भारतीय विशिष्ट पहचान प्राधिकरण द्वारा दी गई सूचना के अनुसार, इसके द्वारा बनाए गए आधार डाटाबेस से इस तरह के किसी भी उल्लंघन की सूचना नहीं मिली है ।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) ने अवगत कराया है कि आधार इकोसिस्टम के बाहर से उनके द्वारा एकत्र की गई निवासियों की आधार से संबंधित जानकारी प्रकाशित करने वाली वेबसाइटों के कुछ उदाहरण सामने आए हैं। रिपोर्ट किए जाने पर ऐसे मामलों में कानून के अनुसार कार्रवाई की जाती है।

(ख) और (ग) : प्रश्न ही नहीं उठता है।

(घ): सरकार ने साइबर सुरक्षा की स्थिति में सुधार करने और ऐसे उल्लंघनों को रोकने के लिए निम्नलिखित प्रतिउपाय किए हैं:

(i) डेटा उल्लंघन या डेटा लीक की घटना का अवलोकन करने पर, सर्ट-इन प्रभावित संगठनों को की जाने वाली उपचारात्मक कार्रवाइयों के साथ सूचित करता है और प्रभावित संगठनों, सेवा प्रदाताओं, संबंधित क्षेत्र के नियामकों के साथ-साथ कानून प्रवर्तन एजेंसियों के साथ घटना प्रतिक्रिया उपायों का समन्वय करता है।
(ii) सर्ट-इन निरंतर आधार पर कंप्यूटर, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों/सुभेद्यताओं और प्रतिउपायों पर चेतावनी और परामर्शी निदेश जारी करता है।
(iii) केंद्र/राज्य सरकारों के सभी मंत्रालयों और विभागों और उनके संगठनों और महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए सर्ट-इन द्वारा तैयार की गई साइबर संकट प्रबंधन योजना साइबर हमलों और साइबर आतंकवाद का मुकाबला करने में मदद करती है।
(iv) सर्ट-इन सूचना प्रौद्योगिकी अवसंरचना को सुरक्षित करने और साइबर हमलों को कम करने के संबंध में नेटवर्क और प्रणाली प्रशासकों और सरकार और महत्वपूर्ण क्षेत्र के संगठनों के मुख्य सूचना सुरक्षा अधिकारियों के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित करता है।

(v) सभी सरकारी वेबसाइटों और एप्लिकेशनों का साइबर सुरक्षा के संबंध में ऑडिट किया जाता है और वेबसाइटों को होस्ट करने से पहले भारत सरकार के दिशानिर्देशों का अनुपालन किया जाता है।

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

(vii) सर्ट-इन सभी क्षेत्रों के संगठनों के साथ उनके द्वारा सक्रिय खतरे को कम करने की कार्रवाइयों के लिए एकत्रित, विश्लेषण और साझा की गई चेतावनी हेतु सक्रिय रूप से एक स्वचालित साइबर खतरा विनिमय मंच संचालित करता है।

(viii) सर्ट-इन दुर्भावनापूर्ण कार्यक्रमों का पता लगाने और उन्हें हटाने के लिए नि:शुल्क उपकरण तथा नागरिकों और संगठनों के लिए साइबर सुरक्षा युक्तियाँ और श्रेष्ठ पद्धतियां प्रदान करने हेतु साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर) का संचालन करता है।

******