सोशल मीडिया और निजिता

संदर्भ

हाल ही के एक घटनाक्रम में फेसबुक से डाटा चोरी होने के बाद अब सारी कंपनियाँ सतर्क हो गई हैं और यही वजह है कि लोग अपने सभी सोशल या दूसरे एकाउंट्स के पासवर्ड बदल रहे हैं। इन घटनाक्रमों को देखते हुए माइक्रो ब्लॉगिंग साइट ट्विटर ने भी दुनिया भर के अपने करोड़ों यूजर्स से अपना पासवर्ड बदलने को कहा है। इन सभी घटनाक्रमों ने पुनः डिजिटल डेटाबेस की गोपनीयता और सुरक्षा को एक प्रमुख राष्ट्रीय चिंता के रूप में उभारा है।

निजिता को बनाए रखने हेतु आवश्यक कदम

- वर्तमान परिदृश्य भारत को डिजिटल सेवाओं के लिये एक नवीन डिज़ाइन तैयार करने का एक अनूठा अवसर प्रदान करते हैं, जिसमें व्यक्तिगत और राष्ट्रीय सुरक्षा दोनों का समावेश हो।
- हमें अमेरिका की तरह क्षेत्र-विशिष्ट मानकों की तुलना में कठोर डाटा संरक्षण संबंधी प्रावधानों को अपनाना चाहिये, क्योंकि वहाँ फेसबुक और गूगल जैसी बड़ी कंपनियों के बावजूद डाटा चोरी की दर सर्वाधिक है।
- और न ही यूरोपियन यूनियन के आदर्शवादी नियमों, जी.डी.पी.आर. (General Data Protection Regulation-GDPR) जो व्यक्ति की निजिता की सुरक्षा से संबंधित हैं, को अपनाना चाहिये भारत को अधिक नवाचार-अनुकूल सेट तैयार करना चाहिये।
- ध्यातव्य है कि यूरोपियन यूनियन के नियम जी.डी.पी.आर आवश्यकता से अधिक सख्त है जिसके कारण ये अप्रभावी साबित हो सकते हैं।
- इसके अलावा, हमारे तैयार किये जाने वाले डिज़ाइन का मुख्य फोकस वंचित आबादी विशेषतः संवेदनशील वर्गों के अनुकूल होना चाहिये।
- निजिता संरक्षण, डेटा संरक्षण से जुड़ा विषय है क्योंकि जब कोई व्यक्ति किसी डिजिटल पहचान द्वारा इंटरनेट माध्यम का प्रयोग करता है तो उस दौरान विभिन्न डाटाओं का संग्रह तैयार हो जाता है जिससे बड़ी आसानी से उपयोगकर्त्ता के निजी डाटा को प्राप्त किया जा सकता है।
- अतः डेटा संरक्षण ढाँचे के डिज़ाइन में महत्त्वपूर्ण चुनौती डिजिटलीकरण के उपयोग से दीर्घकालिक रिकॉर्ड को सुरक्षित रखना तथा इसके साथ ही गोपनीयता को बनाए रखना भी है।
- डिजिटलीकरण का सबसे खौफनाक चेहरा जन निगरानी (mass surveillance) का है।
- इससे नागरिकों और राज्य के बीच सत्ता के संतुलन को संभावित रूप से खतरा हो सकता है जो लोकतंत्र के लिये एक बड़ा खतरा बन सकता है।
- इसके अलावा अपारदर्शी नौकरशाही और राज्य दोनों के द्वारा रहस्यमय तरीके सूचनात्मक आत्मनियंत्रण के खोने से अर्थात् सूचनाओं के इच्छित प्रयोग से भी गोपनीयता के हनन का मामला आम है।
- भारत में प्रभावी डेटा संरक्षण के लिये डेटा नियामकों के पदानुक्रम और एक मजबूत नियामक ढाँचे की आवश्यकता होगी, जो जटिल डिजिटल सेटअप और आम सहमति के अलावा हमारे मूल अधिकारों की रक्षा कर सके।
- इसके अलावा गोपनीयता के उल्लंघनों का तुरंत पता लगाना असान कार्य नहीं है और न ही गोपनीयता के उल्लंघन के बाद किसी दंडकारी कार्रवाई के प्रभावी होने की संभावना भी नहीं होती है अतः एक ऑनलाइन आर्किटेक्चर की आवश्यकता है, जो गोपनीयता के हनन से पूर्व ही रोक दे।
- साथ ही दो अन्य मुख्य भूमिका निभाने की ज़रूरत है। पहला अधिकार-आधारित सिद्धांत के आधार पर विभिन्न डेटा प्रोसेसिंग कार्यों के डेटा एक्सेस के हेतु प्राधिकरणों को निर्धारित करने और स्पष्ट रूप से सूचीबद्ध करने के लिये होना चाहिये।
- दूसरी भूमिका यह सुनिश्चित करने के लिये होनी चाहिये कि ऑनलाइन प्रमाणीकरण और प्रस्तुत प्राधिकरणों के सत्यापन के बाद ही डेटा प्राप्त हो सके।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/architecture-for-privacy