

डाटा-सुरक्षा की उचित व्यवस्था हो



नागरिक पहचान पत्र की शुरुआत के साथ ही इसमें निहित नागरिकों की निजी जानकारी की सुरक्षा को लेकर अनेक सवाल उठते रहे हैं। भला हो उच्चतम न्यायालय का, जिसने निजता को मौलिक अधिकार के रूप में स्वीकार करके नागरिकों को, जानकारी की गोपनीयता भंग होने से बचाव के लिए एक सुरक्षा कवच प्रदान कर दिया है। इन सबके होते हुए भी सरकार का दायित्व है कि वह निजता की रक्षा के ढांचे को ही इतना मजबूत बना दे कि कभी उसमें दरार आने की कोई गुंजाइश ही न रहे। इस संदर्भ में अनेक बिंदुओं पर चर्चा करना अहम् हो जाता है।

- ☑ अमेरिका ने जिस प्रकार से गूगल और फेसबुक के निर्माण और फैलाव में निजता की सुरक्षा के लिए कोई खास कदम नहीं उठाए हैं, उससे अलग हटकर हमें कुछ कड़े प्रावधान रखने होंगे।
- ☑ यूरोपियन जनरल डाटा प्रोटेक्शन रेग्यूलेशन (जीडीपीआर) भी हमारे लिए एक उदाहरण हो सकता है। परंतु यह अनावश्यक रूप से प्रतिबंध लगाने वाला है। ये प्रतिबंध कुछ खास प्रभावी नहीं हैं। भारत को एक अलग नवाचार आधारित सेटअप तैयार करना चाहिए, जो कठोर होने के साथ-साथ प्रभावी भी हो।
- ☑ हमारे डिजाइन कुछ ऐसे हों, जो हमारी जनता हमारी जनसंख्या के एक बड़े वंचित भाग के साथ तारतम्य बैठा सके। इस वर्ग के लोग बहुत अधिक जटिल डिजीटल सेटअप का अनुसरण नहीं कर पाएंगे।
- ☑ डिजीटल पहचान वाली योजनाओं के जरिए लोगों द्वारा किए गये आदान-प्रदान के रिकार्ड को लंबे समय तक रखने से निजता की गोपनीयता भंग होने की संभावना अधिक रहती है। पहचान पत्र या आधार से जुड़े अनेक डाटा ऐसे हैं, जिनसे अलग-अलग क्षेत्र में किसी नागरिक की गतिविधि पर नजर रखी जा सकती है।

इसके लिए सबसे अच्छा है कि भागीदारी स्वैच्छिक हो। गोपनीयता की सुरक्षा के लिए आधारभूत सिद्धांतों के रूप में ऑफ्ट-इन और ऑफ्ट-आउट जैसी व्यक्तिगत भागीदारी के प्रावधान की वकालत की जाती रही है। इसमें उपभोक्ता को नोटिस और उसकी सहमति लेने वाला कदम को बहुत प्रभावशाली नहीं पाया गया है। अक्सर होता यह है कि उपभोक्ता 'आई अग्री' वाले विकल्प को बिना पढ़े ही क्लिक कर देने हैं।

☑ भारत में डाटा सुरक्षा को प्रभावी बनाने के लिए एक सशक्त नियमन ढांचा चाहिए। यह ऐसा हो, जो भले ही जटिल डिजिटल सेटअप वाला हो; जिसमें चाहे सहमति के लिए अनेक स्तर रखे जाएं, परंतु वह हमारे मूल अधिकारों की हर हाल में रक्षा करे।

डाटा नियामकों को स्वायत्तता दी जाए, परंतु उनके लिए डाटा-सुरक्षा के ढांचे में भागीदारी की अनिवार्यता हो।

एल्गोरिदम की स्पष्टता के अलावा उन्हें दो अन्य महत्वपूर्ण भूमिका निभानी चाहिए। (1) उन्हें स्वीकृति के अलावा, अलग-अलग डाटा प्रोसेसिंग कार्यक्रमों में डाटा में पहुँच के अधिकार की भी जाँच करनी चाहिए। (2) केवल स्वीकृत, अधिकृत कम्प्यूटर से ऑनलाइन सत्यापन के बाद ही डाटा तक पहुँच बनाई जाए। इसके लिए डाटा नियामक और नियंत्रक को अलग-अलग लॉग तैयार करने होंगे। इन लॉग्स को कोई अनाधिकृत रूप से खोल न सके, ऐसी भी व्यवस्था हो।

डाटा के ऐसे नियमन के लिए तकनीक मौजूद हैं। अब एक डाटा सुरक्षा कानून और नियमन की क्षमता बढ़ाने की इच्छा का होना आवश्यक है।

'द इंडियन एक्सप्रेस' में प्रकाशित सुभाषीष बनर्जी के लेख पर आधारित। 5 मई, 2018

AFEIAS