

पब्लिक फोरम: डेटा सिक्यूरिटी: नेक्स्ट...नेक्स्ट...नेक्स्ट...डेटा आपका नहीं रहा

संदर्भ एवं पृष्ठभूमि

हाल ही में कैम्ब्रिज एनालिटिक्स द्वारा फेसबुक डेटा लीक मामले सामने आने के बाद भारत सरकार यह चाहती है कि देश में चलने वाली सोशल मीडिया और ऐसी तमाम वेबसाइटें जो यूजर का डेटा एकत्र करती हैं, अपने सर्वर भी भारत में ही लगाएँ ताकि उनमें वदेशी हस्तक्षेप की संभावना कम हो जाए।

- वदिति हो कि इस समय इनके अधिकांश सर्वर अमेरिका में लगे हुए हैं और वहाँ अमेरिकी कानून और कुछ अंतरराष्ट्रीय समझौतों के तहत इनका नियमन किया जा सकता है।
- देश में वेबसाइटों के संचालन, सुरक्षा और स्वतंत्रता के लिये अलग से कोई कानून नहीं है, इसीलिये भारत सरकार इसके नियमन के लिये कानून बनाने पर विचार कर रही है।
- गूगल, ट्विटर, फेसबुक, व्हाट्सएप, लिंक्डइन, इंस्टाग्राम, यूट्यूब आदि जैसी जितनी भी बड़ी सोशल मीडिया साइट्स हैं उनमें से किसी का भी सर्वर भारत में नहीं है। अगर इनके सर्वर भारत में लगाए जाते हैं तो डेटा लीक पर कुछ नयितरण किया जा सकता है।

डेटा क्या है?

किसी सूचना को प्राप्त करने के लिये एकत्र की गई सूचनाओं, तथ्यों तथा आँकड़ों का संग्रह डेटा कहलाता है जो व्यवस्थिति और अव्यवस्थिति दोनों तरीकों से इकट्ठा किया जा जाता है।

- डेटा (Data) का अर्थ है किसी भी तरह की जानकारी या सूचना यानी इनफार्मेशन
- डेटा किसी भी रूप में हो सकता है, जैसे-फाइल, ऑडियो-वीडियो, फोटो, टेक्स्ट, इत्यादि
- सरल शब्दों में कहें तो संगृहीत की हुई कोई भी जानकारी अपने प्रारंभिक रूप में डेटा कहलाती है
- यह डेटा किसी भी तथ्य के बारे में हो सकता है, जैसे-वस्तु, नाम, विचार, स्थान, गुण आदि

सर्वर क्या है?

- सर्वर वह कंप्यूटर प्रोग्राम या कंप्यूटर मशीन है जो अनुरोध आने पर उस पर कार्यवाही कर अनुरोध करने वाले को जवाब देती है।
- किसी भी सर्वर का उद्देश्य उसके उपयोगकर्ताओं के बीच डेटा या हार्डवेयर और सॉफ्टवेयर संसाधनों को साझा करना होता है।
- सामान्यतया सर्वर के रूप में बड़े-बड़े शक्तिशाली कंप्यूटरों का प्रयोग किया जाता है, जिन पर डेटा और अन्य प्रोग्राम इनस्टॉल कर उन्हें नेटवर्क से जोड़ दिया जाता है।
- फरि नेटवर्क से जुड़े अन्य लोग उस सर्वर पर उपलब्ध सूचनाओं और सेवाओं का लाभ उठा सकते हैं।

इसे एक उदाहरण से और अधिक स्पष्ट करते हैं:

यूट्यूब एक ऐसा सर्वर है, जिस पर लाखों की संख्या में वीडियो अपलोड कर रखे गए हैं। जब भी आप यूट्यूब पर जाकर अपनी पसंद का वीडियो देखना चाहते हैं तो उसका सर्वर उस वीडियो को आपके मोबाइल/कंप्यूटर पर भेज देता है।

नेक्स्ट...नेक्स्ट...नेक्स्ट का है कमाल! (Trick Consent)

- अधिकांश यूजर को यह पता ही नहीं होता कि सोशल मीडिया कंपनियों उनके बारे में कतिना जानती हैं। जैसे कि फेसबुक का बिजनेस मॉडल उसके डेटा की गुणवत्ता पर आधारित है और वह इस डेटा को वजिआपनदाताओं को बेचता है और आपको पता नहीं चलता।
- फेसबुक डेटा लीक मामले के बाद से विभिन्न सोशल मीडिया साइटों पर लोग अब प्राइवसी पॉलिसी पढ़ने लगे हैं और अपने एकाउंटों की सेटिंग में सुरक्षा प्रबंध भी कर रहे हैं।
- दरअसल डेटा के दुरुपयोग का आरोप भले ही सोशल साइटों पर लग रहा हो, लेकिन उसके लिये हम भी कम जम्मेदार नहीं हैं।
- सोशल मीडिया वेबसाइटें इस बारे में हमारी सहमतिपिहले ही ले लेती हैं कि यूजर की जानकारी उनके पास रहेगी और वे कहाँ-कहाँ इसका उपयोग कर सकती हैं।
- जब हम सोशल मीडिया पर अपना एकाउंट बना रहे होते हैं तो धड़ाधड़ बना कोई एग्रीमेंट पढ़े, नेक्स्ट...नेक्स्ट...नेक्स्ट...करते हुए आगे बढ़ते जाते हैं तथा पूछी गई जानकारी बेधड़क बताते जाते हैं।

- इंटरनेट की तकनीकी भाषा में इसे ट्रकि कंसेंट कहा जाता है, क्योंकि यूजर को यह पता ही नहीं होता कि उनकी इस सहमति का क्या अर्थ है।

सर्टिफ़ाइड डेटा

एक नागरिक का (Citizen's) डेटा क्या होता है? यदि उसकी दैनिकी पर गौर करें तो वह रोज़ डेटा तैयार करता है। खाने-पीने, सोचने, हंसने, बोलने, रशिते नभाने, सामान खरीदने, डॉक्टर से मिलने, बैंक जाने, राजनीतिक कार्यक्रमों में हिस्सा लेने आदि-आदि। आज तकनीक इतनी सक्षम है कि वह किसी भी नागरिक की सभी गतिविधियों पर नगिरानी रख सकती है। इस तकनीक के लिये हर चीज़ एक डेटा है... एक प्रोडक्ट है, लेकिन नागरिक को डेटा में तब्दील करने का आशय इसके अलावा और कुछ नहीं हो सकता कि उसकी नजिता उसके नियंत्रण में न रहकर नगिरानी में रहे, जबकि एक नागरिक का अपना एक स्वतंत्र जीवन है और वह लगातार उसे बेहतर बनाने की आकांक्षा रखता है।

(टीम दृष्टि इनपुट)

फ़ेसबुक ने किये सुरक्षा उपाय

जब आप किसी भी सोशल मीडिया का उपयोग करते हैं, तो आप अपने डेटा के प्रति विश्वस्त होते हैं कि उसका दुरुपयोग नहीं होगा, जबकि वह उसे कैसे एकत्र करते हैं और उसका उपयोग कैसे करते हैं, इसके बारे में आपको कुछ पता ही नहीं होता।

कैम्ब्रिज एनालिटिक्स द्वारा फ़ेसबुक डेटा लीक मामले के उसके अधिकतर यूजर (सात करोड़) अमेरिका में हैं, लेकिन फ़िलीपींस, इंडोनेशिया और ब्रिटेन में भी 10-10 लाख से अधिक यूजर हैं। अपने यूजर के डेटा की सुरक्षा के लिये फ़ेसबुक अपने सभी 2.2 अरब फ़ेसबुक यूजर को 'प्रोटेक्टिंग योर इंफ़ॉर्मेशन' नाम से एक नोटिस एक लॉक के साथ भेजना शुरू किया है। इससे वे कौन सा एप इस्तेमाल करते हैं और उन ऐप्स पर उन्होंने क्या जानकारी साझा की है इसकी जानकारी मिलेगी। अगर वे चाहें तो अलग-अलग एप को बंद कर सकते हैं या तीसरे पक्ष के देखल को पूरी तरह रोकने के लिये पूरी तरह उसे बंद कर सकते हैं ताकि उनसे जुड़ी किसी जानकारी पर किसी और की पहुँच संभव न हो पाए।

तीसरे पक्ष के पास ऐसे जाता है डेटा

आमतौर पर देखने में आता है कि सोशल साइट्स पर लोग कुछ ऐप्स के परिणाम शेयर करते हैं जिसमें बताया गया होता है कि आपका अच्छा समय कब से शुरू होने वाला है, आप कब अमीर बनने वाले हैं, आपका सबसे करीबी दोस्त कौन है, आपकी शकल किस सेलेब्रिटी से मिलती है, आपकी मृत्यु कब होगी या पछिले जन्म में आप क्या थे... और ऐसा ही बहुत कुछ।

- लोग बिना सोचे समझे सामने वाले का परिणाम देखने के बाद खुद के बारे में भी पता लगाने के लिये उस पर क्लिक कर बैठते हैं और यही से हो जाती है मुश्किल की शुरुआत।
- एप आपको भले यह कहे कि जब तक आप शेयर नहीं करेंगे यह परिणाम आपको ही दिखाएगा लेकिन उसने आपको आपका परिणाम दिखाने के लिये आपसे जो डेटा ले ली है उससे उसका काम तो हो गया।
- जब आप फ़ेसबुक या किसी अन्य साइट पर किसी खास एड मोबाइल के एड पर बार-बार लाइक किया है तो आपको ज़्यादातर के एड मोबाइल फोन के ही दिखाई देंगे।
- यदि आप घूमने-फरिने के स्टेटस अपडेट करते हैं तो आपको ट्रैवल साइटों के विज्ञापन भी दिखाई देंगे।

मोबाइल एप्स को दी जाने वाली परमिशन

- एप इंस्टॉल करने के दौरान कंपनियां आपसे कैमरा, माइक्रोफोन, मेसेज पढ़ने, कॉल डिटिल्स देखने और लोकेशन समेत कई जानकारी लेने के लिये इजाजत मांगती हैं।
- आप जल्दी से एप इंस्टॉल करने के चक्कर में यह नहीं देखते कि आपसे क्या मांगा जा रहा है।
- इसका नुकसान यह होता है कि ये कंपनियां एप के जरिए हर वक्त आप पर नजर बनाए रखती हैं और समय-समय पर उस डेटा का इस्तेमाल अपने नज्दी फायदे के लिये करती हैं।
- मोबाइल एप्स बड़ी आसानी से आपसे अनुमति ले लेते हैं और आपका डेटा इकट्ठा करते रहते हैं। ये एप आपकी हर गतिविधि पर नजर रखते हैं और आपको पता भी नहीं चलता। आप कहां जा रहे हैं, किस कॉल कर रहे हैं, किसके साथ बैठे हैं और किस रेस्तरां में खाना खा रहे हैं, जैसी सारी जानकारी इनकी नज़र में होती है।

एंड्रॉयड फ़्रेमवर्क में आमतौर पर दो तरह की अनुमति होती हैं: नॉर्मल परमिशन और सेंसिटिवि परमिशन।

- नॉर्मल परमिशन के लिये एप आपसे अनुमति नहीं मांगते बल्कि एप इंस्टॉल करते ही यह उन्हें मलि जाती है।
- वाई-फ़ाई, ब्लूटूथ, वॉलपेपर और अलार्म जैसी चीजें इसमें आती हैं, जबकि कैमरा, लोकेशन, माइक्रोफोन और स्टोरेज सहित कई तरह के हार्डवेयर स्टोरेज की इजाजत आपसे मांगी जाती है।
- आप एप इंस्टॉल करते वक्त यह अनुमति भी देते हैं क्योंकि कई एप्स बिना इन परमिशन के डाउनलोड ही नहीं होते।
- अनुमति देने का मतलब है कि आपने उन्हें चाबी दे दी है, अब जैसा मन करेगा, कंपनियां वैसे ही डेटा का इस्तेमाल कर सकती हैं।
- इसमें सबसे खतरनाक बात यह है कि आपको डेटा चोरी के बारे में पता भी नहीं चलेगा, क्योंकि आपके अनुमति देने के बाद एंड्रॉयड फ़्रेमवर्क भी उन्हें आपका डेटा लेने से नहीं रोकता।

कैसे बचें?

- फेसबुक पर कुछ ऐसी फोटो होती हैं, जसि अपने दोस्तों तक ही सीमति रखना चाहते हैं या किसी चीज़ को दूसरों के साथ साझा नहीं करना चाहते।
- फेसबुक की प्राइवैसी सेटिंग्स में जाकर यह तय कथिा जा सकता है कौन आपके पोस्ट्स के साथ ही आपके प्रोफाइल की नजिी जानकारियों, जैसे-फोन नंबर, ईमेल, पता आदि देखे।
- कई लोग फेसबुक पर अपनी नजिी जानकारी को पब्लिक कर देते हैं, जबकयिह सही नहीं है। फेसबुक पर जन्मदिनि, कॉन्टैक्ट नंबर और एड्रेस आदि को पब्लिक न करें तो बेहतर है।
- यदपि सेटोर से कोई एप डाउनलोड करते हैं तो वही सावधान रहना है। हर एप को किसी खास काम के लयि डाउनलोड करते हैं इसलयि हर चीज की अनुमति उसे न दें।
- अगर कोई रेस्तरां का एप है तो उसे कैमरा या मेसेज ऐक्सेस का कोई काम नहीं है। वही अगर कोई पेमेंट एप है तो वह लोकेशन एक्सेस क्यों जानना चाहता है, इस बारे में भी सोचें।
- आपने पहले से कई एप डाउनलोड कयि होंगे, आप उनकी भी परमशिन का रवियू कर सकते हैं। आप देख सकते हैं ककौन-कौन से एप आपसे क्या जानकारी ले रहे हैं।

पासवर्ड की मज़बूती ज़रूरी

- इनके अलावा अपने पासवर्ड बनाते समय स्पेशल कैरक्टर्स का ज़रूर इस्तेमाल करें
- हर अकाउंट के लयि अलग पासवर्ड रखें। महीने, दो महीने में पासवर्ड बदलते रहें
- हर बार नया पासवर्ड बनाएं और स्पेशल कैरक्टर्स ज़रूर रखें
- अपने जन्मदिनि या मोबाइल नंबर को अपना पासवर्ड न बनाएँ
- पासवर्ड बनाते समय सकिर्यूरटि सवाल और जवाब को ज्यादा मज़बूत रखने की कोशशि करें ताकअन्य कोई उसका अनुमान न लगा सके।

सरकारी स्तर पर क्या कथिा जा सकता है?

- बगि डेटा प्रौद्योगिकी (BDT) का उपयोग करने वाली कंपनयियों के लयि भारत को एक अत्याधुनिक सुपर-बगि डेटा केंद्र बनाना चाहयि।
- हमें बगि डेटा प्रौद्योगिकी से संबंधति कंपनयियों को सब्सिडी प्रदान करनी चाहयि, जैसे-सस्ती बजिली, अचल संपत्ति और सस्ता नेटवर्क बैंडविड्थ इत्यादि।
- अलपावर्ध के लयि हमें एक नीतगित ढाँचा भी तैयार करना चाहयि जो हमारी राष्ट्रीय भौगोलिक सीमाओं के भीतर एकत्रति कयि गए डेटा को बनाए रखने के लयि वदिशी बहुराष्ट्रीय कंपनयियों जैसे गूगल और अमेज़न को भारत में अपने बड़े डेटा केंद्रों के नरिमाण को प्रोत्साहति करे।
- हमें हमारे शैक्षणिक और अनुसंधान संस्थानों को बगि डेटा साइंस और डेटा सेंटर प्रौद्योगिकी के क्षेत्र में अनुसंधान और वकिस गतविधियों को बढ़ावा देने हेतु प्रोत्साहति करना चाहयि।

चीन से सीखें

चीन ने इस खतरे को स्पष्ट रूप से समझते हुए सावधानीपूर्वक कदम उठाए हैं। चीन ने बैदू (Baidu) और अलीबाबा जैसी दुनयिा की सबसे बड़ी इंटरनेट कंपनयियों को प्रोत्साहन दयिा है। चीन में गूगल काम करता तो है, लेकिन चीन की तय की हुई शर्तों पर; और न ही बैन होने के बाद फेसबुक वहाँ चलता है। चीन ने कई बड़ी इंटरनेट कंपनयियों को यह नरिदेश दयिा है कवि अपना डेटा चीन में ही सरवर लगाकर स्टोर करें। ऑनलाइन सेंसरशिप में नाकाम रहने पर सुरक्षा का हवाला देते हुए चीन ने वॉट्सएप, ट्विटर और इंस्टाग्राम को भी आंशिक रूप से प्रतबिंधति कयिा हुआ है। चीन के अपने मैसेजगि प्लेटफॉर्म वीचैट के करीब 490 मिलियन एक्टवि यूजरस हैं, जबकवॉट्सएप का इस्तेमाल करने वालों की संख्या केवल 2 मिलियन है।

डेटा सुरक्षा के लयि कानून ज़रूरी

नजिी एवं सार्वजनिक साझेदारी वाली परयिोजनाओं से जुड़े वविादों के नपिटान के लयि बेहतर प्रणाली, उद्योगों के सहयोग से उभरती हुई तकनीकों के प्रयोग, डेटा सुरक्षा के लयि कानूनी ढाँचे की मज़बूती जैसे क्षेत्रों में सरकार को सुधार करने की आवश्यकता है ताककार्य योजना को कारगर तरीके से लागू कथिा जा सकें। शरीक्षण समति की रिपोर्ट के आधार पर भारत में पहली बार नजिता (प्राइवैसी) की परभिषा तय की जा रही है। बदले माहौल में प्राइवैसी का वह मतलब नहीं रह गया है जैसा कयिह कुछ दशक पहले था। साथ यह तमाम सोशल साइट्स का इस्तेमाल करने वाले करोड़ों ग्राहकों को यह भरोसा देगा कउनसे जुड़ी सूचना का कोई गलत इस्तेमाल नहीं कथिा जाएगा।

भारत सरकार इस कानून को ग्राहकों के डेटा को सुरक्षति रखने के मामले में दुनयिा का सर्वश्रेष्ठ कानून बनाना चाहती है। यह कानून सोशल साइट्स पर ही नहीं, बल्ककिसी भी इलेक्ट्रॉनिकस माध्यम में इस्तेमाल होने वाले ग्राहकों से जुड़ी जानकारी को सुरक्षति रखने का ढांचा देगा। यह कानून संचार कंपनयियों पर भी लागू होगा और इससे फोन कंपनयियों की तरफ से ग्राहकों से जुड़ी सूचना को किसी दूसरी एजेंसी को देने पर रोक लगेगी। सरकार का मानना है कभारतीय अर्थव्यस्था का जसि तरह से डिजिटलीकरण हो रहा है उसे देखते हुए एक मजबूत डेटा प्रोटेक्शन कानून बेहद ज़रूरी है।

कुछ वर्ष पूर्व केंद्र सरकार ने तत्कालीन योजना आयोग के तत्वावधान में नजिता पर वशिषज्जों का एक समूह गठति कयिा था। इस वशिषज्ज समूह ने अपनी रिपोर्ट में नजिता की सुरक्षा से जुड़ी चतिाओं के लयि एक रूपरेखा का प्रस्ताव दयिा था। इस वशिषज्ज समूह ने जो रूपरेखा सुझाई थी उसके पाँच प्रमुख आधार थे--

- अंतरराष्ट्रीय मानकों की तकनीकी तटस्थता और अंतर-सक्रयिता,
- बहुआयामी नजिता,
- सरकारी और गैर-सरकारी संस्थाओं को समस्तरीय प्रयोज्यता,
- नजिता सिद्धांतों के साथ अनुरूपता,

- एक सह-नियामक प्रवर्तन व्यवस्था ।

(टीम दृष्टि इनपुट)

नष्टिकर्ष: जैसे-जैसे स्मार्टफोन का चलन बढ़ा है, उसी अनुपात में सोशल नेटवर्कगि साइट्स का इस्तेमाल भी सहज हो गया है। वर्तमान समय को नज्जी कंपनयियों के ऑकड़ों का युग कहा जाता है, क्योकि सोशल मीडिया से लेकर ई-मेल सेवाओं और संदेश भेजने वाले एप्स के माध्यम से बहुत बड़े स्तर पर सूचनाओं का प्रचार-प्रसार होता है। अलग-अलग समूह के लोगों को सोशल नेटवर्कगि साइट्स के इस्तेमाल के जरएि एक मंच पर लाना बेहद आसान हो गया है। ऐसे लोग या समूह जो आपस में कभी मल्लि नहीं, वे भी सोशल नेटवर्कगि साइट के जरएि आपस में आभासी रूप से मल्लि रहे हैं। इन सोशल नेटवर्कगि साइटों का सदस्य बनते समय सभी को अपने वषिय में नज्जी जानकारी देनी होती है और अपनी नज्जी जदिगी से जुड़ी चीजों को शेयर करते हैं। यही जानकारी हमसे पूछे बना कसिी तीसरे पक्ष से शेयर कर दी जाती है, जसिका दुरुपयोग भी हो जाता है। हालाँकि फेसबुक ने कहा है कविह लोगों के डेटा की सुरक्षा के प्रता गंभीर है और उसने अमेरिका और ब्रटिन के अखबारों में वज्जापन देकर इस लीक के लयि माफी भी मांगी है, लेकिन लोगों को यह समझने की ज़रूरत है कयिद कोई वेबसाइट हमें सारी चीज मुफ्त में दे रही है तो भी हम उसके ग्राहक ही हैं और ग्राहक को कीमत कसिी-न-कसिी रूप में चुकानी ही पड़ती है।

PDF Refernece URL: <https://www.drishtias.com/hindi/printpdf/data-security>

