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

संदर्भ एवं पृष्ठभूमि

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

- विदित 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 नियंत्रण 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 व्यवस्थित और अव्यवस्थित दोनों तरीकों से इकठ्ठा 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 उपयोगकर्त्ताओं 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।
- फिर नेटवर्क से जुड़े अन्य लोग उस सर्वर पर उपलब्ध सूचनाओं और सेवाओं का लाभ उठा सकते हैं।

इसे एक उदहारण 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 यूज़र्स को यह पता ही नहीं होता कि सोशल मीडिया कंपनियाँ उनके बारे में कितना जानती हैं। जैसे कि फेसबुक का बिज़नेस मॉडल उसके डेटा की गुणवत्ता पर आधारित है और वह इस डेटा को विज्ञापनदाताओं को बेचता है और आपको पता नहीं चलता।
- फेसबुक डेटा लीक मामले के बाद से विभिन्न सोशल मीडिया साइटों पर लोग अब प्राइवेसी 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 जिम्मेदार नहीं हैं।
- सोशल मीडिया वेबसाइटें इस बारे में हमारी सहमति पहले ही ले लेती हैं कि यूज़र 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 बिना 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 ट्रिक कंसेंट कहा जाता है, क्योंकि यूज़र्स को यह पता ही नहीं होता कि उनकी इस सहमति का क्या अर्थ है।

सिटीज़ंस डेटा

एक नागरिक का (Citizen's) डेटा क्या होता है? यदि उसकी दिनचर्या पर गौर करें तो वह रोज़ डेटा तैयार करता है। खाने-पीने, सोचने, हंसने, बोलने, रिश्ते निभाने, 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 निगरानी 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 निजता उसके नियंत्रण में न रहकर निगरानी में रहे, जबकि एक नागरिक का अपना एक स्वतंत्र जीवन है और वह लगातार उसे बेहतर बनाने की आकांक्षा रखता है।

(टीम दृष्टि इनपुट)

फेसबुक ने किये सुरक्षा उपाय

जब आप किसी भी सोशल मीडिया का उपयोग करते हैं, तो आप अपने डेटा के प्रति विश्विस्त 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 एनालिटिका द्वारा फेसबुक डेटा लीक मामले के उसके अधिकतर यूज़र्स (सात करोड़) अमेरिका में हैं, लेकिन फिलीपींस, इंडोनेशिया और ब्रिटेन में भी 10-10 लाख से अधिक यूज़र्स हैं। अपने यूज़र्स के डेटा की सुरक्षा के लिये फेसबुक अपने सभी 2.2 अरब फेसबुक यूजर्स को 'प्रोटेक्टिंग योर इंफर्मेशन' नाम से एक नोटिस एक लिंक 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 दखल 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 एप्स 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 शक्ल किस सेलेब्रेटी से मिलती है, आपकी मृत्यु कब होगी या पिछले 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 यहीं से हो जाती है मुश्किल की शुरुआत।
- एप आपको भले यह कहे कि जब तक आप शेयर नहीं करेंगे यह परिणाम आपको ही दिखेगा लेकिन उसने आपको आपका परिणाम दिखाने के लिये आपसे जो डिटेल ले ली है उससे उसका काम तो हो गया।
- जब आप फेसबुक 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-फिरने के स्टेटस अपडेट करते हैं तो आपको ट्रैवल साइटों के विज्ञापन भी दिखाई देंगे।

मोबाइल एप्स को दी जाने वाली परमीशन

- एप इंस्टॉल करने के दौरान कंपनियां आपसे कैमरा, माइक्रोफोन, मेसेज पढ़ने, कॉल डिटेल्स देखने और लोकेशन समेत कई जानकारियां 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 निजी 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, किसे कॉल कर रहे हैं, किसके साथ बैठे हैं और किस रेस्तरां में खाना खा रहे हैं, जैसी सारी जानकारी इनकी निगाह में होती है।

एंड्रॉयड फ्रेमवर्क में आमतौर पर दो तरह की अनुमति होती हैं: नॉर्मल परमीशन और सेंसिटिव परमीशन।

- नॉर्मल परमीशन के लिये एप आपसे अनुमति नहीं मांगते बल्कि एप इंस्टॉल करते ही यह उन्हें मिल जाती है।
- वाई-फाई, 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 दे 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, कंपनियाँ 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 एंड्रायड फ्रेमवर्क भी उन्हें आपका डेटा लेने से नहीं रोकता।

कैसे बचें?

- फेसबुक पर कुछ ऐसी फोटो होती हैं, जिसे अपने दोस्तों तक ही सीमित रखना चाहते हैं या किसी चीज़ को दूसरों के साथ साझा नहीं करना चाहते।
- फेसबुक की प्राइवेसी सेटिंग्स में जाकर यह तय किया जा सकता है कौन आपके पोस्ट्स के साथ ही आपके प्रोफाइल की निजी जानकारियों, जैसे-फोन नंबर, ईमेल, पता आदि देखे।
- कई लोग फेसबुक पर अपनी निजी जानकारी को पब्लिक कर देते हैं, जबकि यह सही नहीं है। फेसबुक पर जन्मदिन, कॉन्टैक्ट नंबर और एड्रेस आदि को पब्लिक न करें तो बेहतर है।
- यदि प्ले स्टोर से कोई एप डाउनलोड करते हैं तो वहीं सावधान रहना है। हर एप को किसी खास काम के लिये डाउनलोड करते हैं इसलिये हर चीज की अनुमति उसे न दें।
- अगर कोई रेस्तरां का एप है तो उसे कैमरा या मेसेज ऐक्सेस का कोई काम नहीं है। वहीं अगर कोई पेमेंट एप है तो वह लोकेशन एक्सेस क्यों जानना चाहता है, इस बारे में भी सोचें।
- आपने पहले से कई एप डाउनलोड किये होंगे, आप उनकी भी परमिशन का रिव्यू कर सकते हैं। आप देख सकते हैं कि कौन-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 लिये अलग पासवर्ड रखें। महीने, दो महीने में पासवर्ड बदलते रहें
- हर बार नया पासवर्ड बनाएं और स्पेशल कैरक्टर्स ज़रूर रखें
- अपने जन्मदिन या मोबाइल नंबर को अपना पासवर्ड न बनाएँ
- पासवर्ड बनाते समय सिक्यूरिटी सवाल और जवाब को ज्यादा मज़बूत रखने की कोशिश करें ताकि अन्य कोई उसका अनुमान न लगा सके।

सरकारी स्तर पर क्या किया जा सकता है?

- बिग डेटा प्रौद्योगिकी (BDT) का उपयोग करने वाली कंपनियों के लिये भारत को एक अत्याधुनिक सुपर-बिग डेटा केंद्र बनाना चाहिये।
- हमें बिग डेटा प्रौद्योगिकी से संबंधित कंपनियों को सब्सिडी प्रदान करनी चाहिये, जैसे-सस्ती बिजली, अचल संपत्ति और सस्ता नेटवर्क बैंडविड्थ इत्यादि।
- अल्पावधि के लिये हमें एक नीतिगत ढाँचा भी तैयार करना चाहिये जो हमारी राष्ट्रीय भौगोलिक सीमाओं के भीतर एकत्रित किये गए डेटा को बनाए रखने के लिये विदेशी बहुराष्ट्रीय कंपनियों जैसे गूगल और अमेज़न को भारत में अपने बड़े डेटा केंद्रों के निर्माण को प्रोत्साहित करे।
- हमें हमारे शैक्षणिक और अनुसंधान संस्थानों को बिग डेटा साइंस और डेटा सेंटर प्रौद्योगिकी के क्षेत्र में अनुसंधान और विकास गतिविधियों को बढ़ावा देने हेतु प्रोत्साहित करना चाहिये।

चीन से सीखें

चीन ने इस खतरे को स्पष्ट रूप से समझते हुए सावधानीपूर्वक कदम उठाए हैं। चीन ने बैदू (Baidu) और अलीबाबा जैसी दुनिया की सबसे बड़ी बड़ी इंटरनेट कंपनियों को प्रोत्साहन दिया 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 कंपनियों को यह निर्देश दिया है कि वे अपना डेटा चीन में ही सर्वर 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 प्रतिबंधित किया हुआ है। चीन के अपने मैसेजिंग प्लेटफॉर्म वीचैट के करीब 490 मिलियन एक्टिव यूजर्स हैं, जबकि वॉट्सएप का इस्तेमाल करने वालों की संख्या केवल 2 मिलियन है।

डेटा सुरक्षा के लिये कानून ज़रूरी

निजी एवं सार्वजनिक साझेदारी वाली परियोजनाओं से जुड़े विवादों के निपटान के लिये बेहतर प्रणाली, उद्योगों के सहयोग से उभरती हुई तकनीकों के प्रयोग, डेटा सुरक्षा के लिये कानूनी ढाँचे की मज़बूती जैसे क्षेत्रों में सरकार को सुधार करने की आवश्यकता है ताकि कार्य योजना को कारागर तरीके से लागू किया जा सकें। श्रीकृष्ण समिति की रिपोर्ट के आधार पर भारत में पहली बार निजिता (प्राइवेसी) की परिभाषा तय की जा रही है। बदले माहौल में प्राइवेसी का वह मतलब नहीं रह गया है जैसा कि यह कुछ दशक पहले था। साथ यह तमाम सोशल साइट्स का इस्तेमाल करने वाले करोड़ों ग्राहकों को यह भरोसा देगा कि उनसे जुड़ी सूचना का कोई गलत इस्तेमाल नहीं किया जाएगा।

भारत सरकार इस कानून को ग्राहकों के डेटा को सुरक्षित रखने के मामले में दुनिया का सर्वश्रेष्ठ कानून बनाना चाहती है। यह कानून सोशल साइट्स पर ही नहीं, बल्कि किसी भी इलेक्ट्रॉनिक्स माध्यम में इस्तेमाल होने वाले ग्राहकों से जुड़ी जानकारी को सुरक्षित रखने का ढांचा देगा। यह कानून संचार कंपनियों पर भी लागू होगा और इससे फोन कंपनियों की तरफ से ग्राहकों से जुड़ी सूचना को किसी दूसरी एजेंसी को देने पर रोक लगेगी। सरकार का मानना है कि भारतीय अर्थव्यस्था का जिस तरह से डिजिटिलीकरण हो रहा है उसे देखते हुए एक मजबूत डेटा प्रोटेक्शन कानून बेहद जरूरी है।

कुछ वर्ष पूर्व केंद्र सरकार ने तत्कालीन योजना आयोग के तत्वावधान में निजिता पर विशेषज्ञों का एक समूह गठित किया था। इस विशेषज्ञ समूह ने अपनी रिपोर्ट में निजिता की सुरक्षा से जुड़ी चिंताओं के लिये एक रूपरेखा का प्रस्ताव दिया था। इस विशेषज्ञ समूह ने जो रूपरेखा सुझाई थी उसके पाँच प्रमुख आधार थे--

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

- एक सह-नियामक प्रवर्तन व्यवस्था।

(टीम दृष्टि इनपुट)

निष्कर्ष: जैसे-जैसे स्मार्टफोन का चलन बढ़ा है, उसी अनुपात में सोशल नेटवर्किंग साइट्स का इस्तेमाल भी सहज हो गया है। वर्तमान समय को निजी कंपनियों के आँकड़ों का युग कहा जाता है, क्योंकि 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 नेटवर्किंग साइट्स के इस्तेमाल के जरिए एक मंच पर लाना बेहद आसान हो गया है। ऐसे लोग या समूह जो आपस में कभी मिले नहीं, वे भी सोशल नेटवर्किंग साइट के ज़रिये आपस में आभासी रूप से मिल रहे हैं। इन सोशल नेटवर्किंग साइटों का सदस्य बनते समय सभी को अपने विषय में निजी जानकारी देनी होती है और अपनी निजी जिंदगी से जुड़ी चीजों को शेयर करते हैं। यही जानकारी हमसे पूछे बिना किसी तीसरे पक्ष से शेयर कर दी जाती हैं, जिसका दुरुपयोग भी हो जाता है। हालाँकि फेसबुक ने कहा है कि वह लोगों के डेटा की सुरक्षा के प्रति गंभीर है और उसने अमेरिका और ब्रिटेन के अखबारों में विज्ञापन देकर इस लीक के लिये माफी भी मांगी है, लेकिन लोगों को यह समझने की ज़रूरत है कि यदि कोई वेबसाइट हमें सारी चीज मुफ्त में दे रही है तो भी हम उसके ग्राहक ही हैं और ग्राहक को कीमत किसी-न-किसी रूप में चुकानी ही पड़ती है।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/data-security