

कृत्रिम बुद्धिमत्ता के युग में डिजिटल गोपनीयता

डॉ. सुरभि पांडे

प्राध्यापक, आईआईपीए (IIPA)

एआई में डिजिटल गोपनीयता को समझना

डिजिटल गोपनीयता का अर्थ है डिजिटल दुनिया में व्यक्तिगत डेटा, पहचान और व्यवहार संबंधी जानकारी की सुरक्षा। एआई (AI) के संदर्भ में गोपनीयता की चिंता इसलिए बढ़ जाती है क्योंकि:

- **एआई सिस्टम बड़े स्तर पर डेटा एकत्र करते हैं।**
- अलग-अलग प्लेटफॉर्म से उपयोगकर्ताओं का डेटा इकट्ठा किया जाता है।
- व्यवहार संबंधी जानकारी (जैसे क्लिक करना, सर्च करना, स्क्रॉल करना) एकत्र की जाती है।
- डै-पार्टी (तीसरे पक्ष) के डेटा को भी जोड़ा जाता है।

- डेटा में व्यक्तिगत पहचान संबंधी जानकारी, बायोमेट्रिक जानकारी, ब्राउज़िंग व्यवहार, स्थान संबंधी जानकारी तथा वित्तीय लेन-देन शामिल होते हैं।

व्यक्तिगत पहचान संबंधी जानकारी :

नाम, आधार नंबर, ईमेल, फोन नंबर

बायोमेट्रिक डेटा: चेहरे की तस्वीर, उंगलियों के निशान, आईरिस स्कैन, आवाज़ का पैटर्न

व्यवहार संबंधी डेटा: ब्राउज़िंग हिस्ट्री, खरीदारी की आदतें, ऑनलाइन गतिविधियां

स्थान संबंधी डेटा: रीयल-टाइम जीपीएस ट्रैकिंग, आने-जाने का रिकॉर्ड

वित्तीय डेटा: लेन-देन का रिकॉर्ड, क्रेडिट हिस्ट्री, लोन से जुड़ी जानकारी

- **स्वचालित निर्णय-प्रक्रिया (Automated decision-making)** लोगों के अधिकारों, सुविधाओं और अवसरों को प्रभावित करती है।
 - लोन की स्वीकृति
 - बीमा प्रीमियम तय करना
 - भर्ती प्रक्रिया में चयन
 - सरकारी कल्याण योजनाओं के लिए पात्रता
 - कानून प्रवर्तन एजेंसियों द्वारा निगरानी/लक्षित कार्रवाई

एआई प्रणालियों में गोपनीयता जोखिम के प्रमुख तत्व

- **डेटा संग्रह (Data Collection)**
 - आवश्यकता से अधिक डेटा एकत्र करना
 - सूचित सहमति (Informed Consent) का अभाव
 - कुकीज़ या ऐप्स के माध्यम से निष्क्रिय ट्रैकिंग (बिना स्पष्ट जानकारी के निगरानी)
- **डेटा प्रसंस्करण (Data Processing)**
 - मूल उद्देश्य से परे डेटा का द्वितीयक उपयोग
 - एल्गोरिदम के माध्यम से संवेदनशील विशेषताओं का अनुमान लगाना
 - विभिन्न स्रोतों से डेटा को एकत्रित कर जोड़ना
- **डेटा भंडारण (Data Storage)**

जोखिम कारक:

- केंद्रीकृत डेटाबेस
- क्लाउड सुरक्षा में कमजोरियाँ
- कमजोर एन्क्रिप्शन मानक

- **डेटा साझाकरण (Data Sharing)**

- तृतीय-पक्ष विक्रेताओं (Third-party vendors) के साथ डेटा साझा करना
- सीमा-पार डेटा स्थानांतरण
- डेटा ब्रोकर नेटवर्क/प्रणाली

- **स्वचालित प्रोफाइलिंग (Automated Profiling)**

जोखिम कारक:

- व्यवहार आधारित लक्षित विज्ञापन/निशाना बनाना
- पूर्वानुमान आधारित जोखिम स्कोरिंग
- उपयोगकर्ताओं का सूक्ष्म-विभाजन (Micro-segmentation)

एआई गोपनीयता जोखिमों को क्यों बढ़ाता है?

कृत्रिम बुद्धिमत्ता (AI) केवल डेटा को संग्रहित नहीं करती, बल्कि उससे अर्थ निकालती है, भविष्यवाणियाँ करती है और निर्णयों को स्वचालित रूप से लेती है। यही कारण है कि पारंपरिक डिजिटल प्रणालियों की तुलना में एआई गोपनीयता जोखिमों को अधिक बढ़ा देता है।

एआई प्रणालियाँ :

- बड़े पैमाने पर डेटा से पैटर्न सीखती हैं।
- संवेदनशील जानकारी (जैसे धर्म, स्वास्थ्य स्थिति, राजनीतिक पसंद) का अनुमान लगा सकती हैं।
- पूर्वानुमान आधारित प्रोफाइलिंग (Predictive Profiling) को सक्षम बनाती हैं।
- निर्णयों को बड़े स्तर पर स्वतः लागू करती हैं।

उदाहरण (Examples):

- चेहरे की पहचान आधारित निगरानी (Facial Recognition Surveillance)
- एआई आधारित क्रेडिट स्कोरिंग
- पूर्वानुमान आधारित पुलिसिंग (Predictive Policing)
- स्वास्थ्य जोखिमों की भविष्यवाणी

भारत में एआई और डिजिटल गोपनीयता को नियंत्रित करने वाला कानूनी एवं नीतिगत ढांचा

- डिजिटल पर्सनल डेटा प्रोटेक्शन अधिनियम, 2023 (DPDP Act)
- सूचना प्रौद्योगिकी अधिनियम, 2000
- राष्ट्रीय कृत्रिम बुद्धिमत्ता रणनीति (नीति आयोग)
- इंडिया एआई मिशन (IndiaAI Mission)
- संवैधानिक संरक्षण (गोपनीयता का अधिकार एक मौलिक अधिकार के रूप में)

एआई के उपयोग के मामले एवं गोपनीयता के निहितार्थ

- **स्वास्थ्य क्षेत्र में एआई (Healthcare AI):** एआई आधारित निदान प्रणाली मरीजों के रिकॉर्ड का विश्लेषण करती है।

जोखिम: संवेदनशील स्वास्थ्य संबंधी डेटा के उजागर होने की संभावना।

उदाहरण: एआई द्वारा कैंसर के जोखिम की भविष्यवाणी करना।

- **वित्तीय क्षेत्र में एआई (Financial AI)**

- क्रेडिट स्कोरिंग एल्गोरिदम

जोखिम: पक्षपातपूर्ण (भेदभावपूर्ण) स्वचालित प्रोफाइलिंग

- **सोशल मीडिया में एआई (Social Media AI)**

- कंटेंट सुझाव (Recommendation) प्रणाली
- जोखिम:** व्यवहार आधारित ट्रैकिंग

- **स्मार्ट सिटी एवं निगरानी (Smart Cities & Surveillance)**

- चेहरे की पहचान (Facial Recognition)
- रीयल-टाइम ट्रैकिंग
- बड़े पैमाने पर डेटा संग्रह

एआई में वास्तविक दुनिया की गोपनीयता चुनौतियाँ

- डेटा उल्लंघन (Data Breaches)
- डीपफेक और पहचान की चोरी
- बिना सहमति के डेटा स्क्रेपिंग
- एल्गोरिदमिक पक्षपात और भेदभाव
- शैडो प्रोफाइलिंग (बिना जानकारी के प्रोफाइल बनाना)

- **उदाहरण :**
- उपयोगकर्ता की अनुमति के बिना सोशल मीडिया की तस्वीरों को एआई द्वारा स्क्रेप करना।
- आवाज़ की नकल (Voice Cloning) का दुरुपयोग।

एआई में डिजिटल गोपनीयता के लिए उपकरण

- **व्यक्तिगत स्तर के उपकरण (Personal Level Tools)**

- एंड-टू-एंड एन्क्रिप्टेड मैसेजिंग (जैसे: Signal)
- गोपनीयता-केंद्रित ब्राउज़र (जैसे: Brave, Tor)
- पासवर्ड मैनेजर (जैसे: Bitwarden)
- वीपीएन (VPN) सेवाएँ

- **संगठनात्मक स्तर के उपकरण (Organisational Tools)**

- डेटा अनामीकरण (Anonymization) सॉफ़्टवेयर
- एआई मॉडल ऑडिटिंग उपकरण
- गोपनीयता प्रभाव आकलन (Privacy Impact Assessment) रूपरेखाएँ
- डेटा लॉस प्रिवेंशन (DLP) प्रणाली

एआई युग में डिजिटल साक्षरता

व्यक्तियों को यह समझना आवश्यक है:

डेटा कैसे एकत्र किया जाता है

एआई प्रणालियाँ क्या निष्कर्ष निकालती हैं

गोपनीयता सेटिंग्स को कैसे प्रबंधित करें

फ़िशिंग और डीपफेक खतरों को पहचानना

सहमति प्रपत्र (Consent Forms) को समझना

डिजिटल साक्षरता गोपनीयता की रक्षा की पहली पंक्ति है।

धन्यवाद ...