

# उभरती प्रौद्योगिकियों में गोपनीयता जोखिम

डिजिटल पारिस्थितिकी में विश्वास, नियंत्रण और शासन की आवश्यकता

प्रस्तुतकर्ता :  
अंशुल टेलर  
परियोजना अभियंता

कार्यक्रम : सी.आई.ई.टी – एन.सी.ई.आर.टी एवं ISEA-सी-डैक द्वारा आयोजित ऑनलाइन प्रशिक्षण

# मुख्य बिंदु

- प्राइव्हेसी
- प्राइव्हेसी पैराडॉक्स
- उभरती प्रौद्योगिकियों
- मानव व्यवहार
- डेटा आधारित अर्थव्यवस्था
- संरचना स्तर पर रक्षा
- अनुपालन
- निष्कर्ष

# प्राइवेसी क्या है?

- प्राइवेसी वह अधिकार है जिसके अंतर्गत व्यक्ति यह नियंत्रित कर सकता है कि उसकी व्यक्तिगत जानकारी कब, कैसे और किस उद्देश्य से उपयोग की जाए।
- प्राइवेसी के मुख्य तत्व:



नियंत्रण

डेटा पर अंतिम अधिकार  
उपयोगकर्ता का



सहमति

स्पष्ट रूप से दिया गया,  
सूचित निर्णय



उद्देश्य-सीमा

डेटा केवल घोषित उद्देश्य  
के लिए



पारदर्शिता

उपयोगकर्ता जानता हो कि  
डेटा कहाँ जा रहा है

# प्राइवैसी क्यों महत्वपूर्ण है?

प्राइवैसी सुरक्षा, स्वतंत्रता और विश्वास की नींव है।

यह इसलिए महत्वपूर्ण है क्योंकि:

- यह व्यक्ति की पहचान और स्वायत्तता की रक्षा करता है
- डेटा के गलत उपयोग और हेरफेर से बचाता है
- डिजिटल अधिकारों को सुरक्षित करता है
- साइबर अपराध, धोखाधड़ी और प्रोफाइलिंग का जोखिम कम करता है
- उपयोगकर्ता को अपने डिजिटल जीवन पर नियंत्रण देता है

# प्राइवेसी क्यों महत्वपूर्ण है?

लोग प्राइवेसी के बारे में क्या सोचते हैं?

अधिकांश लोग कहते हैं:

- मैं अपनी प्राइवेसी का ध्यान रखता हूँ।
- मैं कोई निजी जानकारी साझा नहीं करता।
- मैं केवल सुरक्षित ऐप्स का उपयोग करता हूँ।
- मैं अपनी डिजिटल सुरक्षा को लेकर जागरूक हूँ।

लेकिन यह केवल धारणा है, वास्तविकता नहीं।

वास्तविकता क्या है?

व्यवहार वास्तविकता में कुछ और है:

- बिना पढ़े “Accept All” क्लिक करना।
- ऐप्स को अनावश्यक परमिशन देना।
- सोशल मीडिया पर अत्यधिक जानकारी साझा करना।
- सार्वजनिक Wi-Fi पर संवेदनशील काम करना।

यही वह अंतर है जहाँ प्राइवेसी जोखिम पैदा होते हैं।

# प्राइव्हेसी पैराडॉक्स

“हम कहते कुछ हैं, करते कुछ और हैं।”

प्राइव्हेसी पैराडॉक्स का सार:

लोग प्राइव्हेसी की चिंता व्यक्त करते हैं लेकिन वही लोग ऐसी गतिविधियाँ करते हैं जो उनकी प्राइव्हेसी को कमजोर करती हैं।

यह मानव व्यवहार और तकनीकी वास्तविकता का टकराव है।



# तकनीक कैसे प्राइवैसी जोखिम बढ़ाती है?

उभरती प्रौद्योगिकियाँ मानव व्यवहार में मौजूद कमजोरियों को गुणात्मक रूप से बढ़ा देती हैं ।

मुख्य कारण:

- निरंतर निगरानी
- डेटा का अत्यधिक संग्रह
- स्वचालित प्रोफाइलिंग
- एल्गोरिदमिक निर्णय
- कंपनियों का डेटा-चालित बिज़नेस मॉडल

# उभरती प्रौद्योगिकियों का तीव्र विस्तार

कृत्रिम बुद्धिमत्ता एवं मशीन  
लर्निंग

अनुमान लगाने की शक्ति

IoT एवं स्मार्ट स्पेस

हर जगह मौजूद, हमेशा चालू डेटा संग्रह

बायोमेट्रिक्स

स्थायी और अपरिवर्तनीय पहचानकर्ता

एजेंटिक AI

उपकरणों तक पहुँच के साथ स्वायत्त निर्णय लेने वाली प्रणालियाँ

# प्राइवैसी परिदृश्य में कृत्रिम बुद्धिमत्ता का प्रभाव

- कृत्रिम बुद्धिमत्ता प्राइवैसी को कई गुना अधिक जटिल बना देता है
- उच्च-स्तरीय अनुमान लगाने की क्षमता
  - सार्वजनिक डेटा से छिपे हुए गुण/विशेषताएँ उजागर करना
  - री-आइडेंटिफिकेशन: Anonymized डेटा को भी संभावित रूप से वापस पहचान में बदला जा सकता है

# IoT और स्मार्ट स्पेसेज़

- आपका स्मार्ट स्पीकर आपकी बातें सुनता है
- आपकी कार आपकी हर लोकेशन जानती है
- आपका फिटनेस ट्रैकर आपकी नींद की आदतें जानता है
- हमेशा चालू डेटा संग्रह
  - घर और शहर अब डेटा फैक्टरी की तरह काम करते हैं
- व्यवहार-आधारित बायोमेट्रिक्स
  - चाल-ढाल, आवाज़ के पैटर्न, टाइपिंग रिदम
  - कमजोर सुरक्षा के कारण ये डिवाइसेज़ अक्सर हमलावरों के लिए सबसे आसान प्रवेश बिंदु बन जाते हैं

# बायोमेट्रिक्स और पहचान

- अपरिवर्तनीय पहचानकर्ता
  - बायोमेट्रिक्स अभूतपूर्व सुविधा प्रदान करते हैं, लेकिन एक बार समझौता हो जाए तो उसे बदला नहीं जा सकता।
  - आप लीक हुआ पासवर्ड बदल सकते हैं, लेकिन.....
- निगरानी जोखिम
- स्पूफिंग और दुरुपयोग
  - डीपफेक चेहरों से फेस-ID धोखा देना
  - फिंगरप्रिंट/वाँइस की नकल करके अनधिकृत एक्सेस



# मानव व्यवहार जो जोखिम बढ़ाता है

गोपनीयता को सबसे अधिक नुकसान हमारी स्वयं की डिजिटल आदतों से होता है।

“सब स्वीकार करें” संस्कृति

सुविधा को सावधानी से अधिक महत्व

कम डिजिटल जागरूकता

तकनीक पर अंधविश्वास

# नीति और शासन की कमज़ोरियाँ

तकनीक बहुत तेजी से बदल रही है, लेकिन नियम और नियंत्रण उसके अनुरूप तेज़ी से विकसित नहीं हो पा रहे।



धीमी नियम निर्माण प्रक्रिया

कमज़ोर सहमति व्यवस्था

कम पारदर्शिता

ज़िम्मेदारी की अस्पष्टता

# डेटा आधारित अर्थव्यवस्था : बढ़ते जोखिम का मुख्य कारण

आज डेटा सबसे मूल्यवान संसाधन बन चुका है। जितना अधिक डेटा, उतना अधिक लाभ — और यही गोपनीयता के लिए सबसे बड़ा खतरा है।

- निगरानी आधारित अर्थव्यवस्था
- बिना मूल्य वाली सेवाएँ, पर डेटा की भारी कीमत
- अधिक डेटा संग्रह की प्रवृत्ति
- कृत्रिम बुद्धिमत्ता को विशाल डेटा की आवश्यकता

# उपयोगकर्ता क्या कर सकते हैं

- ऐप की अनुमतियाँ सावधानी से दें
- मजबूत सुरक्षा कोड और दो-स्तरीय सुरक्षा अपनाएँ
- व्यक्तिगत जानकारी कम से कम साझा करें
- संदिग्ध संदेश और कड़ियों से सावधान रहें
- समय-समय पर प्राइवैसी की जाँच करें
- सार्वजनिक जाल (वाई-फाई) पर संवेदनशील काम न करें

सार:

जागरूक उपयोगकर्ता ही पहली सुरक्षा पंक्ति हैं।

# संरचना स्तर पर रक्षा

## डिज़ाइन द्वारा प्राइवेसी

प्रणाली की मूल संरचना में ही प्राइवेसी नियंत्रण शामिल हों।

## डेटा न्यूनता

जितना आवश्यक हो केवल उतना ही डेटा प्रवाह हो।

## सुदृढ़ अभिगम नियंत्रण

कौन क्या देख सकता है, उसका सख्त निर्धारण।

## उच्च स्तरीय कूटलेखन

डेटा का संचरण एवं संग्रह दोनों चरण सुरक्षित रहे।

## विभक्त संरचना

जोखिम फैलने से रोकने के लिए डेटा और सिस्टम अलग-अलग।

# अनुपालन

## डीपीडीपी अधिनियम 2023 (भारत)

- स्पष्ट सहमति
- न्यूनतम डेटा संग्रह
- उपयोगकर्ता के अधिकार
- डेटा प्रबंधन करने वाले पर पूर्ण जवाबदेही

## आइएसओ 27701 (प्राइवैसी प्रबंधन मानक)

- डेटा संग्रह, उपयोग और सुरक्षा के लिए नियंत्रित ढाँचा
- नियमित समीक्षा और सुधार
- स्पष्ट भूमिकाएँ और जिम्मेदारियाँ

## निस्ट प्राइवैसी ढाँचा

- जोखिम आधारित प्राइवैसी प्रबंधन
- पहचान, नियंत्रण, शासन और संरक्षण के सिद्धांत
- उभरती तकनीकों के लिए व्यावहारिक मार्गदर्शन

सार: अनुपालन केवल कानूनी आवश्यकता नहीं एक मज़बूत रक्षा तंत्र है।

# निष्कर्ष

- प्राइवेटि कोई सीमित सुविधा नहीं है; यह निरंतर जिम्मेदारी है।
- हमें “हम पर भरोसा करें” से आगे बढ़कर।
- “सुनिश्चित करें कि आपका डेटा सुरक्षित है” की संस्कृति अपनानी होगी।
- कृत्रिम बुद्धिमत्ता जोखिम भी बढ़ाएगी और समाधान भी।

**धन्यवाद !**  
आपके समय और सहभागिता के लिए आभार।

**प्रश्न एवं चर्चा स्वागत योग्य हैं।**