व्यक्तिगत रूप से पहचान योग्य सूचना की संरक्षा

प्रिलिम्स के लिये:

व्यक्तिगत रूप से पहचान योग्य सूचना, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In), सोशल इंजीनियरिंग अटैक, निजता, साइबर अपराध, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023, विस्तारित पहचान और प्रतिक्रिया (XDR) उपकरण

मेन्स के लिये:

डेटा उल्लंघन, साइबर अपराध से संबंधित चुनौतियाँ और इससे निपटने के उपाय

स्रोत: द हिंदू

चर्चा में क्यों?

हाल ही में एक साइबर सुरक्षा शोधकर्त्ता ने भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In) को एक गंभीर सुभेद्यता के बारे में सूचना दी जिसके बाद **कारपोरेट कार्य मंत्रालय (Ministry of Corporate Affairs)** ने अपने ऑनलाइन पोर्टल में सुधार किया।

- कथित तौर पर सूचित सुभेद्यता के कारण भारतीय कंपनियों के 98 लाख से अधिक निदेशकों का आधार, स्थायी खाता संख्या (PAN), मतदाता पहचान, जन्म तिथि, संपर्क नंबर तथा संचार पते जैसी व्यक्तिगत रूप से पहचान योग्य सूचना (PII) संबंधी डेटा लीक हुआ।

व्यक्तिगत रूप से पहचान योग्य सूचना (PII) क्या है?

- **परिचय:**
  - PII किसी **संगठन अथवा एजेंसी द्वारा अनुरक्षित** कोई भी **डेटा अथवा सूचना** है जिसका उपयोग संभावित रूप से किसी विशिष्ट व्यक्ति की पहचान करने के लिये किया जा सकता है।
    - इसमें **आधार, PAN, मतदाता पहचान, पासपोर्ट, जन्म तिथि, संपर्क नंबर**, संचार पता और बायोमेट्रिक जानकारी जैसी विभिन्न सूचनाएँ शामिल हो सकती है।
  - PII के घटक किसी **व्यक्ति के निवास देश** के आधार पर भिन्न-भिन्न होते हैं।
- **PII के प्रकार:**
  - PII के दो प्रकार होते हैं: **प्रत्यक्ष पहचानकर्त्ता और अप्रत्यक्ष पहचानकर्त्ता।**
    - **प्रत्यक्ष पहचानकर्त्ता** किसी व्यक्ति के संबंध में **अद्वितीय** होते हैं जिसमें पासपोर्ट नंबर अथवा ड्राइविंग लाइसेंस नंबर जैसी चीज़ें शामिल होती हैं।
      - प्रत्यक्ष पहचानकर्त्ता आमतौर पर किसी की पहचान निर्धारित करने के लिये पर्याप्त होता है।
    - अप्रत्यक्ष पहचानकर्त्ता अद्वितीय नहीं होते हैं तथा इनमें जाति और जन्म स्थान जैसे अधिक सामान्य व्यक्तिगत विवरण शामिल होता है। **मात्र एक अप्रत्यक्ष पहचानकर्त्ता सूचना के माध्यम से किसी व्यक्ति की पहचान नहीं की जा सकती** किंतु अप्रत्यक्ष पहचानकर्त्ता संबंधी विभिन्न सूचना के माध्यम से ऐसा किया जा सकता है।
- **संवेदनशील बनाम गैर-संवेदनशील PII:**
  - PII में कुछ सूचना अन्य सूचनाओं की तुलना में अधिक संवेदनशील होती हैं।
  - **संवेदनशील PII:**
    - यह संवेदनशील सूचना होती है जिसके माध्यम से **प्रत्यक्ष रूप से किसी व्यक्ति की पहचान** की जा सकती है तथा इसके लीक अथवा चोरी होने की दशा में **गंभीर क्षति** हो सकती है।
    - संवेदनशील PII आम तौर पर सार्वजनिक रूप से उपलब्ध नहीं होती है और अधिकांश मौजूदा डेटा गोपनीयता संबंधी कानूनों के आधार पर संगठनों को इस डेटा को एन्क्रिप्ट करके, इसे एक्सेस करने वाले को नियंत्रित करने अथवा अन्य साइबर सुरक्षा उपाय करके इसे सुरक्षित रखने की आवश्यकता होती है।
  - **गैर-संवेदनशील PII:**
    - यह **किसी व्यक्ति के संबंध में अद्वितीय हो भी सकता है और नहीं भी।**

            ◦ यह व्यक्तिगत डेटा होता है जो लीक अथवा चोरी होने पर किसी व्यक्ति को गंभीर क्षति नहीं पहुँचाता है।
        - उदाहरण के लिये किसी व्यक्ति का **सोशल मीडिया अकाउंट गैर-संवेदनशील** PII की श्रेणी में आता है। यह किसी व्यक्ति की पहचान करने में मदद सकता है किंतु कोई दुर्भावनापूर्ण अभिकर्त्ता केवल सोशल मीडिया अकाउंट नाम के माध्यम से संबद्ध व्यक्ति की पहचान की चोरी नहीं कर सकता है।
        - इसमें **ज़िप कोड, जाति, लिंग तथा धर्म** जैसी जानकारी भी शामिल होती है जिनका उपयोग किसी व्यक्ति की सटीक पहचान करने के लिये नहीं किया जा सकता है।

- **Non-PII:**
    - Non-PII सूचना में फोटोग्राफिक छवियाँ (विशेष रूप से मुख अथवा व्यक्ति की अन्य पहचान से संबंधित), जन्म स्थान, धर्म, भौगोलिक संकेतक, रोज़गार की जानकारी, शैक्षिक योग्यता और चिकित्सा रिकॉर्ड शामिल होते हैं।
        - **गैर-व्यक्तिगत रूप से पहचान योग्य सूचना (Non-PII)** वह डेटा है जिसका उपयोग किसी **व्यक्ति का पता लगाने अथवा उसकी पहचान करने के लिये** नहीं किया जा सकता है। हालाँकि **अतिरिक्त सूचना** और Non-PII **का उपयोग कर किसी व्यक्ति की पहचान की जा सकती है।**

PII के गोपीनयता से जुड़े जोखिम क्या हैं?

- **वित्तीय धोखाधड़ी:**
    - PII के खुलासा, जैसे **बैंक खाता संख्या या क्रेडिट कार्ड की जानकारी, वित्तीय धोखाधड़ी का कारण** बन सकती है।
        - अपराधी बैंक खातों तक पहुँच सकते हैं, अनधिकृत लेन-देन कर सकते हैं, **भुगतान संबंधी धोखाधड़ी** कर सकते हैं, साथ ही सरकारी **कल्याण कार्यक्रमों** के **लाभार्थियों को आवंटित खातों से धनराशि** निकाल सकते हैं, जिसके परिणामस्वरूप पीड़ित को वित्तीय हानि हो सकती है।
- **गोपनीयता का उल्लंघन:**
    - **PII** का खुलासा **गोपनीयता का उल्लंघन** **कर सकता है साथ ही व्यक्तियों की गोपनीयता और स्वायत्तता से भी समझौता कर सकता है।**
        - व्यक्तिगत डेटा तक अनधिकृत पहुँच द्वारा **गोपनीयता का हनन, उत्पीड़न अथवा पीड़ितों का पीछा भी** शामिल है।
- **फिशिंग तथा सोशल इंजीनियरिंग हमले:**
    - साइबर अपराधी **फिशिंग हमलों** को अंज़ाम देने, व्यक्तियों की अधिक **संवेदनशील जानकारी का खुलासा करने अथवा दुर्भावनापूर्ण लिंक** पर क्लिक करने के लिये **PII के खुलासे** का उपयोग कर सकते हैं।
        - सोशल इंजीनियरिंग हमले, जैसे- हेरफेर PRAKRI तथा प्रतिरूपण धोखाधड़ी, लोगों को निजी जानकारी का खुलासा करने अथवा अवैध पहुँच की अनुमति देने के लिये उजागर की गई व्यक्तिगत पहचान योग्य जानकारी (PII) का उपयोग करते हैं।
- **डेटा उल्लंघन का परिणाम:**
    - PII का खुलासा प्रायः **डेटा उल्लंघनों** के माध्यम से होता है, जिससे महत्त्वपूर्ण वित्तीय हानि के साथ सुधारात्मक लागत और संगठन की प्रतिष्ठा को भी हानि पँहुचाता है।
        - संगठन ग्राहकों के विश्वास में कमी, राजस्व में कमी तथा नियामकों एवं हितधारकों की बढ़ती जाँच से प्रभावित हो सकते हैं।
- **प्रतिष्ठा की हानि:**
    - संवेदनशील PII का खुलासा, जैसे कि आपत्तिजनक तस्वीरें अथवा व्यक्तिगत संदेश, व्यक्तियों की प्रतिष्ठा और रिश्तों को हानि पहुँचा सकते हैं।
        - ऑनलाइन लीक हुई जानकारी का उपयोग **ब्लैकमेल,** जबरन वसूली या **सार्वजनिक अपमान के लिये** किया जा सकता है, जिसके सामाजिक एवं व्यावसायिक परिणाम हो सकते हैं।

अतीत में डेटा उल्लंघन के मामले:

- **CoWIN डेटा उल्लंघन का आरोप:**
    - टेलीग्राम बॉट द्वारा **CoWIN पोर्टल** पर पंजीकृत भारतीय नागरिकों के व्यक्तिगत डेटा को वापस करने के बारे में रिपोर्ट सामने आई।
        - इसी तरह का एक डेटा उल्लंघन तब सामने आया था जब एक **अमेरिकी साइबर सुरक्षा कंपनी** ने दावा किया था कि आधार नंबर और पासपोर्ट विवरण सहित 815 मिलियन **भारतीय नागरिकों की PII डार्क वेब पर बेची** जा रही थी।
        - भारत सरकार ने बायोमेट्रिक डेटा लीक और CoWIN पोर्टल उल्लंघनों के आरोपों से इनकार किया और कहा कि CoWIN वेबसाइट सुरक्षित है साथ ही इसमें डेटा गोपनीयता के लिये पर्याप्त सुरक्षा उपाय हैं।
- **आधार:**
    - वर्ष 2018, 2019 और 2022 में भी आधार डेटा लीक की सूचना मिली थी, जिसमें बड़े पैमाने पर लीक के तीन मामले सामने आए थे, जिनमें से एक में **PM किसान** वेबसाइट पर संग्रहीत किसान डेटा को डार्क वेब पर उपलब्ध कराया गया था।
- **रेलयात्री प्लेटफार्म डेटा का उल्लंघन:**
    - जनवरी 2023 में रेलयात्री प्लेटफॉर्म पर भी डेटा उल्लंघन की सूचना मिली थी।
- **सरकारी एवं आवश्यक सेवाओं पर साइबर हमलों में वृद्धि:**
    - इसके अतिरिक्त **67% भारतीय सरकार और आवश्यक सेवा संगठनों** ने विघटनकारी **साइबर हमलों** में 50% से अधिक की वृद्धि का अनुभव किया जैसा कि रिसिक्योरिटी (एक अमेरिकी साइबर सुरक्षा कंपनी) की एक रिपोर्ट में कहा गया है।
    - इसके अतिरिक्त **200 IT निर्णय निर्माताओं के एक सर्वेक्षण** में कहा गया है कि **45% भारतीय व्यवसायों ने साइबर हमलों में 50% से अधिक की वृद्धि का अनुभव** किया है।

भारत में डेटा गवर्नेंस से संबंधित प्रावधान:

- सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम 2021
- आईटी अधिनियम, 2000 को प्रतिस्थापित करने के लिए ' डिजिटल इंडिया अधिनियम', 2023 का प्रस्ताव
- न्यायमूर्ति के.एस. पुट्टास्वामी (सेवानिवृत्त) बनाम भारत संघ 2017
    - भारत में **निजी डेटा के प्रसंस्करण को नियंत्रित** करता है। यह अधिनियम ऑनलाइन और ऑफलाइन डेटा संग्रह साथ ही प्रसंस्करण दोनों पर लागू होता है, जिसमें भारत के बाहर की गतिविधियाँ भी शामिल हैं, यदि उनमें भारत में सामान या सेवाएँ पेश करना शामिल है।
- **कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In):**
    - **सूचना प्रौद्योगिकी संशोधन अधिनियम 2008** में, CERT-In को साइबर सुरक्षा के क्षेत्र में कई कार्य करने के लिये राष्ट्रीय एजेंसी के रूप में नामित किया गया है, साथ ही साइबर घटनाओं पर जानकारी का संग्रह, विश्लेषण और प्रसार भी साइबर सुरक्षा घटनाओं पर अलर्ट जारी करता है।
        - यह **इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय का एक संगठन** है।
        - **CERT-In के उद्देश्यों में** शामिल हैं: देश के साइबरस्पेस के खिलाफ साइबर हमलों को रोकना, साइबर हमलों का जवाब देना तथा क्षति एवं वसूली को कम करना।

PII की सुरक्षा में क्या चुनौतियाँ हैं?

- **विविध स्रोत:**
    - **क्लाउड कंप्यूटिंग एवं SaaS सेवाओं के विकास के कारण PII को कई स्थानों पर संग्रहीत और संसाधित किया जा सकता है।**
- **डेटा की मात्रा बढ़ाना:**
    - **सार्वजनिक क्लाउड में संग्रहीत संवेदनशील डेटा की मात्रा वर्ष 2024 तक दोगुनी** होने का अनुमान है, जिससे इसकी सुरक्षा सुनिश्चित करने में चुनौतियाँ पैदा होंगी।
- **विकसित हो रहा खतरा:**
    - PII चुराने के लिये साइबर अपराधी विभिन्न तकनीकों का प्रयोग करते हैं, जिनमें सोशल इंजीनियरिंग हमले तथा डार्क वेब पर डेटा खरीदना शामिल है।
- **जटिल विनियामक वातावरण:**
    - संगठनों को विभिन्न डेटा गोपनीयता नियमों का पालन करना चाहिये और उनके अनुसार अपने सुरक्षा उपायों को भी तैयार करना चाहिये।

आगे की राह

- **एन्क्रिप्शन:**
    - PII की सुरक्षा के लिये एन्क्रिप्शन तकनीकों को नियोजित करना, भले ही डेटा की स्थिति कुछ भी हो, चाहे वह डेटाबेस पर हो अथवा इंटरनेट पर पारगमन में हो या उपयोग में हो।
- **पहचान एवं पहुंच प्रबंधन (IAM):**
    - संवेदनशील डेटा तक पहुँच सीमित करने के लिये दो-कारक या बहु-कारक प्रमाणीकरण एवं ज़ीरो-ट्रस्ट आर्किटेक्चर (ZTA) का उपयोग करना।
        - ZTA **"कभी भरोसा न करने, हमेशा सत्यापित करने"** के सिद्धांत पर आधारित है। इसके लिये संगठनों को प्रत्येक उपयोगकर्त्ता की पहचान सत्यापित करने और दुर्भावनापूर्ण गतिविधि के लिये उपयोगकर्ता व्यवहार की लगातार निगरानी करने की आवश्यकता होती है।
- **प्रशिक्षण:**
    - **कर्मचारियों को फिशिंग-विरोधी और सामाजिक इंजीनियरिंग जागरूकता** सहित **PII** को संभालने और सुरक्षा पर प्रशिक्षण प्रदान करना।
- **अज्ञातीकरण:**
    - पहचान संबंधी विशेषताओं को हटाने के लिये संवेदनशील डेटा को अज्ञात बनाना।
- **साइबर सुरक्षा उपकरण:**
    - **DLP** के दुरुपयोग पर नज़र रखने और उसका पता लगाने के लिये**डेटा हानि रोकथाम** (**DLP**) तथा **विस्तारित पहचान एवं प्रतिक्रिया (XDR)** उपकरण तैनात करना।
        - **XDR** उपकरण सुरक्षा उपकरण हैं जो संपूर्ण नेटवर्क से डेटा एकत्र करते हैं और खतरों के लिये स्वचालित प्रतिक्रियाओं का प्रबंधन करते हैं।
- **सहयोग एवं भागीदारी:**
    - व्यक्तिगत रूप से पहचान योग्य जानकारी की सुरक्षा के लिये नए जोखिमों और सर्वोत्तम प्रथाओं पर अपडेट रहने के लिये उद्योग मित्रों, नियामक एजेंसियों तथा साइबर सुरक्षा विशेषज्ञों के साथ मिलकर कार्य करना।

UPSC सविलि सेवा परीक्षा, वगित वर्ष के प्रश्न

[illegible]:

प्रश्न 1. 'नजिता का अधकिार' भारत के संवधािन के कसि अनुच्छेद के तहत संरक्षति है? (2021)

(a)अनुच्छेद 15
(b)अनुच्छेद 19
(c)अनुच्छेद 21
(d)अनुच्छेद 29

व्याख्या: (c)

Q.2 भारत में, साइबर सुरक्षा घटनाओं पर रपिोर्ट करना नम्निलखिति में से कसिके लयि कानूनी रूप से अनवािर्य है? (2017)

1. सेवा प्रदाता
2. डेटा केंद्र
3. बॉडी कॉर्पोरेट

नीचे दयि गए कूट का उपयोग करके सही उत्तर का चयन कीजयि:

(a) केवल 1
(b) केवल 1 और 2
(c) केवल 3
(d) 1, 2 और 3

उत्तर: (d)

[illegible]:

प्रश्न. साइबर सुरक्षा के वभिन्नि तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजयि कि भारत ने कसि हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक वकिसति की है। (2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/safeguarding-personally-identifiable-information