संचार साथी ऐप को अनिवार्य करना: सुरक्षा की आवश्यकता या निजता का अतिक्रमण?

यूपीएससी प्रासंगिकता: **जी.एस. पेपर II, शासन (Governance) और जी.एस. पेपर-3, साइबर सुरक्षा (Cybersecurity)**

ख़बरों में क्यों?

दूरसंचार विभाग (**DoT**) ने स्मार्टफोन निर्माताओं को मार्च 2026 से भारत में बेचे जाने वाले सभी नए उपकरणों पर **संचार साथी ऐप** को **प्री-इंस्टॉल** करने का आदेश दिया है, यह सुनिश्चित करते हुए कि इसकी कार्यक्षमताओं को **अक्षम (disabled) नहीं किया जा सकता** है।

यह निर्देश **डिजिटल गिरफ्तारी घोटाले (Digital Arrest Scams), सिम के दुरुपयोग और स्पूफ्ड IMEI ऑपरेशन** सहित बढ़ते साइबर अपराध को रोकने के उद्देश्य से, **सिम-बाइंडिंग** पर एक समानांतर निर्देश के साथ आया है।

यह निर्देश संचार साथी प्लेटफॉर्म के माध्यम से रिपोर्ट किए गए धोखाधड़ी के बढ़ते मामलों के बाद दिया गया है, जिसने पहले ही **2.48 लाख शिकायतों** और मोबाइल कनेक्शन की जाँच के लिए **2.9 करोड़ अनुरोधों** पर कार्रवाई की है।

पृष्ठभूमि

भारत में साइबर अपराधों में तेज़ी से वृद्धि देखी गई है, जैसे:

- **डिजिटल गिरफ्तारी** (नकली पुलिस/सरकारी कॉल)
- भारतीय नंबरों का उपयोग करके **सीमा पार घोटाले**
- एक साथ विभिन्न स्थानों पर काम कर रहे **स्पूफ्ड IMEI** वाले डिवाइस
- **गुमनाम व्हाट्सएप/टेलीग्राम धोखाधड़ी**
- **सेकंड-हैंड मोबाइल बाजार का दुरुपयोग**, जहाँ चोरी हुए डिवाइस बेचे जाते हैं

इनका मुकाबला करने के लिए, **संचार साथी**—जिसे शुरू में 2023 में एक **केवल-वेब प्लेटफॉर्म** के रूप में लॉन्च किया गया था—को उपयोगकर्ताओं को धोखाधड़ी वाले कॉल की रिपोर्ट करने और मोबाइल कनेक्शन को सत्यापित करने में मदद करने के लिए डिज़ाइन किया गया था, जिसका उद्देश्य **TRAI के DND ऐप** के समान है।

निर्देश के बारे में अधिक जानकारी

1. सिम-बाइंडिंग की आवश्यकता

- यदि सिम हटा दिया जाता है या निष्क्रिय कर दिया जाता है, तो मैसेजिंग/संचार खाते **स्वचालित रूप से समाप्त (auto-terminate)** हो जाने चाहिए।
- इसका उद्देश्य गुमनाम उपयोग को रोकना है, खासकर सीमा पार साइबर धोखाधड़ी अभियानों में।

2. संचार साथी का अनिवार्य प्री-इंस्टॉलेशन

- ऐप को पहली बार बूट होने पर **दिखना** चाहिए।
- कार्यक्षमताओं को **सक्षम और अप्रतिबंधित** रहना चाहिए, जिसमें हटाने का कोई विकल्प न हो।
- यह **त्वरित IMEI सत्यापन**, नकली/ग्रे-मार्केट फोन की पहचान और तेज़ शिकायत समाधान सुनिश्चित करता है।
- यह ऐप डिवाइस रिकवरी का समर्थन करता है, अब यह पोर्टल **मासिक 50,000 से अधिक चोरी हुए डिवाइस** को रिकवर करने में मदद कर रहा है।

3. उद्देश्य और कार्यक्षमता

- **IMEI की प्रामाणिकता** को सत्यापित करना ताकि उपयोगकर्ताओं को गैर-असली या छेड़छाड़ किए गए हैंडसेट से बचाया जा सके।
- दूरसंचार संसाधनों के **संदिग्ध दुरुपयोग की रिपोर्ट** करना।
- **ब्लॉक किए गए/ब्लैकलिस्टेड IMEI** की पहचान करना, जो सेकंड-हैंड डिवाइस बाजार के लिए विशेष रूप से प्रासंगिक है।
- DoT और इसकी Google Play लिस्टिंग के अनुसार, ऐप **उपयोगकर्ता डेटा एकत्र नहीं करता है।**

उठाई गई चिंताएँ

1. राज्य निगरानी की क्षमता (Potential for State Surveillance)

एक प्री-इंस्टॉल्ड, न हटाने योग्य ऐप जिसमें **गहन सिस्टम-स्तरीय एकीकरण** हैं, इससे निम्न का डर पैदा होता है:

- **अत्यधिक राज्य निगरानी**
- निगरानी बुनियादी ढांचे का विस्तार
- पेगासस से जुड़े पिछले आरोपों के समान **दुरुपयोग**, जिसने पत्रकारों और कार्यकर्ताओं को निशाना बनाया था
- हालांकि DoT का दावा है कि ऐप निजता के लिए सुरक्षित है, आलोचकों को डर है कि भविष्य के अपडेट इसकी पहुँच का विस्तार कर सकते हैं।

2. निजता और आनुपातिकता का उल्लंघन (पुट्टास्वामी निर्णय)

सुप्रीम कोर्ट को निजता के सभी अतिक्रमणों को निम्न पर खरा उतरना आवश्यक है:

- **वैधानिकता (Legality)**
- **आवश्यकता (Necessity)**
- **आनुपातिकता (Proportionality)**

आलोचकों का तर्क है कि:

- **कम दखल देने वाले विकल्प** पहले से ही मौजूद हैं (SMS-आधारित जाँच, USSD कोड, वेब पोर्टल)।
- सिस्टम-स्तरीय ऐप को अनिवार्य करना **आनुपातिकता की कसौटी पर खरा नहीं उतरता** है क्योंकि नरम विकल्प (softer options) व्यवहार्य हैं।

3. साइबर सुरक्षा भेद्यता (Cybersecurity Vulnerability)

एक अनिवार्य, उच्च-अनुमति वाला ऐप निम्न बन सकता है:

- **विफलता का एकल बिंदु (A single point of failure)**
- मैलेयर, एक्सप्लॉइट किट या सप्लाई-चेन हमलों का **मुख्य लक्ष्य**
- इस परत पर समझौता होने से एक साथ **लाखों उपयोगकर्ता** खतरे में पड़ सकते हैं।

4. मुक्त बाजार के माहौल में अतिरेक (Overreach in a Free Market Environment)

- अनिवार्य ऐप्स **वैश्विक मानदंडों** से टकराते हैं। स्मार्टफोन निर्माता—विशेष रूप से Apple जैसी निजता-केंद्रित कंपनियाँ—ने ऐतिहासिक रूप से ऐसी आवश्यकताओं का विरोध किया है।
- **उदाहरण:** Apple ने पहले अत्यधिक अनुमतियों के कारण TRAI के DND ऐप का विरोध किया था और अंततः सिस्टम-स्तरीय पहुँच की अनुमति देने के बजाय एक **iMessage-आधारित समाधान** बनाया था।

संभावित प्रभाव:

- उपभोक्ता स्वायत्तता का **क्षरण**
- वैश्विक निर्माताओं को **नकारात्मक संकेत**
- भारत के तकनीकी पारिस्थितिकी तंत्र को प्रभावित करने वाला **नियामक घर्षण**

सरकार का तर्क क्या है

- भारत का **विशाल सेकंड-हैंड फोन बाजार** धोखाधड़ी और चोरी हुए डिवाइस के सर्कुलेशन को सक्षम बनाता है।
- **स्पूफ्ड IMEI** अपराधियों को ट्रैकिंग से बचने और कई उपकरणों का प्रतिरूपण करने की अनुमति देते हैं।
- **सिम-बाइंडिंग** साइबर अपराधियों द्वारा शोषण किए जाने वाले गुमनाम ऑनलाइन व्यवहार को रोकता है।
- एक प्री-इंस्टॉल्ड ऐप **समान सुरक्षा मानकों** को सुनिश्चित करता है।

आगे की राह (Way Forward)

1. कम दखल देने वाले विकल्पों को प्राथमिकता दें

- संचार साथी पोर्टल का उपयोग जारी रखें।
- SMS-आधारित IMEI सत्यापन।
- *#06# जैसे USSD कोड।
- अनिवार्य ऐप के बजाय **वैकल्पिक डाउनलोड करने योग्य** ऐप की पेशकश करें।

2. एक उचित कानूनी ढाँचा पेश करें

- जनादेश केवल DoT के निर्देशों से नहीं, बल्कि **स्पष्ट कानून** से उत्पन्न होने चाहिए।
- **डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम** और SC निजता सिद्धांत के साथ **संरेखित** होना चाहिए।

3. पारदर्शिता सुनिश्चित करें

- ऐप की अनुमतियाँ और डेटा नीतियों को **स्पष्ट रूप से प्रकाशित** करें।
- **स्वतंत्र सुरक्षा ऑडिट** आयोजित करें।
- डेटा पहुँच, प्रतिधारण और उद्देश्य पर **सीमाएँ निर्धारित** करें।

4. उद्योग हितधारकों को शामिल करें

- अनावश्यक घर्षण से बचने के लिए स्मार्टफोन कंपनियों से **परामर्श** करें।
- **राष्ट्रीय सुरक्षा** को नवाचार और उपयोगकर्ता की पसंद के साथ **संतुलित** करें।
- एक **भविष्य कहने योग्य नियामक वातावरण** स्थापित करें।

5. साइबर पुलिसिंग को मजबूत करें

- अंतर-राज्यीय समन्वय में **सुधार** करें।
- घोटाले के हब की मेजबानी करने वाले देशों के साथ **अंतर्राष्ट्रीय सहयोग बढ़ाएँ**।
- डिजिटल फोरेंसिक में पुलिस को **प्रशिक्षित** करें।
- सभी क्षेत्रों में **डिजिटल साक्षरता को बढ़ावा** दें।

निष्कर्ष

भारत एक गंभीर साइबर अपराध संकट का सामना कर रहा है, और दूरसंचार पारिस्थितिकी तंत्र को सुरक्षित करने का सरकार का इरादा **वैध** है। हालाँकि, संचार साथी ऐप को सिस्टम स्तर पर अनिवार्य करना, बिना **ऑप्ट-आउट** के और बिना किसी **स्पष्ट विधायी आधार** के, निम्न का जोखिम उठाता है:

- निजता को **कमजोर करना**
- साइबर सुरक्षा **भेद्यताएँ** पैदा करना
- निगरानी की **चिंताओं को बढ़ाना**
- वैश्विक निर्माताओं के साथ संबंधों में **तनाव पैदा करना**

सुरक्षा उपायों को संवैधानिक अधिकारों से **समझौता नहीं करना चाहिए**। यह सुनिश्चित करने के लिए कि इलाज बीमारी से ज़्यादा ख़तरनाक न हो, एक **संतुलित दृष्टिकोण**—जो **पारदर्शी, आनुपातिक, कानूनी रूप से आधारित और तकनीकी रूप से सुदृढ़** हो—आवश्यक है।

यूपीएससी मुख्य परीक्षा अभ्यास प्रश्न

प्र 1 "संचार साथी ऐप का अनिवार्य प्री-इंस्टॉलेशन भारत के डिजिटल पारिस्थितिकी तंत्र के बढ़ते **सुरक्षीकरण (securitisation)** को दर्शाता है, लेकिन यह **निजता, आनुपातिकता और उपभोक्ता स्वायत्तता** के बारे में भी चिंताएँ पैदा करता है।" दूरसंचार विभाग (DoT) द्वारा जारी हालिया निर्देशों के संदर्भ में चर्चा करें। (150 शब्द)