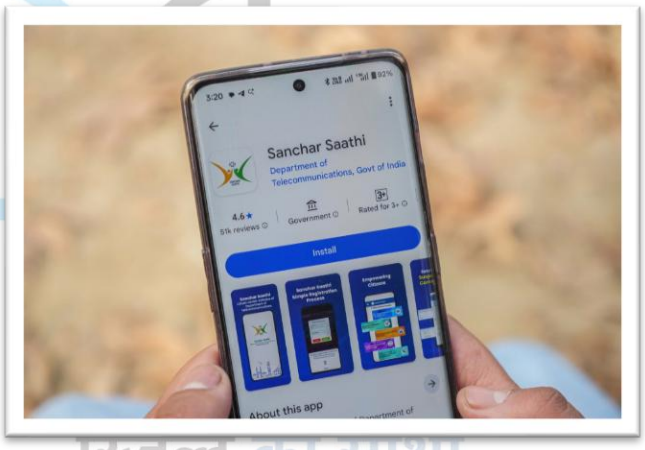
क्या सरकार स्मार्टफोन का सोर्स कोड मांग रही है? राष्ट्रीय सुरक्षा, साइबर सुरक्षा और डिजिटल विश्वास के बीच संतुलन

UPSC प्रासंगिकता:

- **सामान्य अध्ययन प्रश्न पत्र II** – शासन व्यवस्था (Governance), पारदर्शिता और जवाबदेही।
- **सामान्य अध्ययन प्रश्न पत्र III** – आंतरिक सुरक्षा और प्रौद्योगिकी - साइबर सुरक्षा खतरे, आपूर्ति श्रृंखला सुरक्षा (Supply chain security)।

चर्चा में क्यों?



हालिया रिपोर्टों से संकेत मिला है कि भारत सरकार स्मार्टफोन निर्माताओं से उनके 'सोर्स कोड' (Source Code) को तीसरे पक्ष की परीक्षण एजेंसियों के साथ साझा करने और प्रमुख सॉफ्टवेयर अपडेट से पहले अधिकारियों को सूचित करने पर विचार कर रही थी। हालांकि सरकार ने किसी भी अंतिम मांग से इनकार किया है, लेकिन इस मुद्दे ने साइबर सुरक्षा, डिजिटल संप्रभुता, गोपनीयता और नियामक अतिरेक (Regulatory overreach) पर बहस छेड़ दी है।

IAS-PCS Institute
Result
रिजल्ट का साथी
@resultmitra www.resultmitra.com 9235313184, 9235440806

सोर्स कोड क्या है और यह संवेदनशील क्यों है?

सोर्स कोड निर्देशों का वह मूलभूत सेट है जो किसी सॉफ्टवेयर सिस्टम को चलाता है।

- यह परिभाषित करता है कि कोई डिवाइस कैसे कार्य करता है, डेटा कैसे स्टोर करता है और इनपुट पर कैसे प्रतिक्रिया देता है।
- यद्यपि एंड्रॉइड (Android) में ओपन-सोर्स घटक होते हैं, स्मार्टफोन कंपनियां इसमें भारी बदलाव करती हैं, जैसे:
  - मालिकाना सॉफ्टवेयर (Proprietary software)
  - सुरक्षा परतें (Security layers)
  - हार्डवेयर-विशिष्ट अनुकूलन (Optimisations)

कंपनियां सोर्स कोड की सुरक्षा क्यों करती हैं?

- **व्यावसायिक कारण:** इसमें बौद्धिक संपदा (IP) और व्यापारिक रहस्य होते हैं।
- **सुरक्षा कारण:** सोर्स कोड तक पूर्ण पहुंच होने से सिस्टम का अध्ययन करना, उसकी 'रिवर्स-इंजीनियरिंग' करना और हमला करना आसान हो जाता है। अधिकांश साइबर हमले ज्ञात कमजोरियों का फायदा उठाते हैं—खुली पहुंच इन जोखिमों को बढ़ा सकती है।

IAS-PCS Institute

विवाद का कारण क्या था?

1. **रॉयटर्स की रिपोर्ट:** इसमें दावा किया गया कि सरकार अनिवार्य सोर्स कोड प्रकटीकरण और सॉफ्टवेयर अपडेट से पहले अधिसूचना की संभावना तलाश रही है।
2. **अतीत का संदर्भ (संचार साथी ऐप):** दूरसंचार विभाग (DoT) ने पहले फोन निर्माताओं से एक सरकारी ऐप प्री-इंस्टॉल करने को कहा था। इसके कारण जन आक्रोश फैला और निगरानी (Surveillance) व सुरक्षा जोखिमों का डर पैदा हुआ। इस घटना ने हितधारकों को राज्य के हस्तक्षेप के प्रति सतर्क कर दिया।

सरकार का अब तक का रुख

नियामक पृष्ठभूमि: 2023 में, DoT के तहत 'नेशनल सेंटर फॉर कम्युनिकेशन सिक्योरिटी' (NCSS) ने उपभोक्ता उपकरणों के लिए 'भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएं' (ITSARs) तैयार की थीं। ये 'दूरसंचार उपकरणों के अनिवार्य परीक्षण और प्रमाणन' (MTCTE) शासन का हिस्सा थे।

Result Mitra
रिजल्ट का साथी

नीतिगत बदलाव: दूरसंचार अधिनियम, 2023 के बाद, स्मार्टफोन को MTCTE के बजाय इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) और BIS प्रमाणन के तहत स्थानांतरित कर दिया गया। सरकार का दावा है कि:

- अभी तक कोई अंतिम निर्णय नहीं लिया गया है।
- हितधारकों के साथ चर्चा "खुले मन" से जारी है।

पारदर्शिता संबंधी चिंताएं: इंटरनेट फ्रीडम फाउंडेशन (IFF) का तर्क है कि मसौदा (Draft ITSARs) अभी भी सार्वजनिक रूप से उपलब्ध है और बैठकों में पारदर्शिता व सार्वजनिक परामर्श की कमी है।

सोर्स कोड प्रकटीकरण एक बड़ी चिंता क्यों है?

1. साइबर सुरक्षा जोखिम: पूर्ण पहुंच से निम्नलिखित की संभावना बढ़ जाती है:

- प्रणाली की कमजोरियों की खोज।
- मैलवेयर विकास।
- आपूर्ति श्रृंखला हमले (Supply-chain attacks)। *उदाहरण:* विश्व स्तर पर कई साइबर उल्लंघन तीसरे पक्ष या अंदरूनी पहुंच के माध्यम से हुए हैं।

2. गोपनीयता और निगरानी का डर: सिस्टम-स्तरीय कोड तक पहुंच से राज्य द्वारा निगरानी और 'बैकडोर' (Backdoors) बनाने की चिंता पैदा होती है, जिससे डिजिटल उपकरणों में उपयोगकर्ता का विश्वास कमजोर हो सकता है।

3. नवाचार और निवेश पर प्रभाव: वैश्विक कंपनियां भारत में उत्पादों के लॉन्च में देरी कर सकती हैं या कुछ बाजारों से बच सकती हैं। *उदाहरण:* एप्पल (Apple) ने अन्य रियायतों के बावजूद चीन में भी सोर्स कोड देने का विरोध किया है।

4. अंतर्राष्ट्रीय व्यापार और WTO मुद्दे: अनिवार्य प्रकटीकरण बौद्धिक संपदा संरक्षण और व्यापार समझौतों का उल्लंघन कर सकता है। इसे 'गैर-टैरिफ बाधा' के रूप में देखा जा सकता है।

5. नियामक ओवरलैप और भ्रम: कई एजेंसियां (DoT, MeitY, BIS) अनुपालन अनिश्चितता और नीतिगत विखंडन पैदा करती हैं।

सरकार का संभावित तर्क

विवादास्पद होने के बावजूद, सरकार की चिंताएं पूरी तरह निराधार नहीं हैं:

राष्ट्रीय सुरक्षा: छिपी हुई कमजोरियों या विदेशी बैकडोर को रोकना।

- **आपूर्ति श्रृंखला सुरक्षा:** विशेष रूप से भू-राजनीतिक तकनीकी प्रतिद्वंद्विता के बीच।
- **उपभोक्ता संरक्षण:** यह सुनिश्चित करना कि अपडेट सुरक्षा से समझौता न करें।

आगे की राह: एक संतुलित नियामक दृष्टिकोण

1. **पूर्ण प्रकटीकरण के बिना सुरक्षा ऑडिट:** विश्वसनीय एजेंसियों द्वारा नियंत्रित ऑडिट की अनुमति दी जाए, न कि सोर्स कोड तक पूर्ण पहुंच।

2. **पारदर्शी सार्वजनिक परामर्श:** नियमों के मसौदे जारी करें और नागरिक समाज, शिक्षाविदों और साइबर सुरक्षा विशेषज्ञों को शामिल करें।
3. **स्वतंत्र परीक्षण को मजबूत करना:** बाइनरी टेस्टिंग, पेनेट्रेशन टेस्टिंग और भेद्यता प्रकटीकरण कार्यक्रमों (Vulnerability disclosure programmes) पर ध्यान केंद्रित करें।
4. **स्पष्ट नियामक क्षेत्राधिकार:** DoT, MeitY और BIS के बीच ओवरलैप से बचें। उपभोक्ता उपकरणों के लिए एक मुख्य नियामक होना चाहिए।
5. **विश्वास-आधारित डिजिटल गवर्नेंस:** विनियमन को सुरक्षा, गोपनीयता और नवाचार को बढ़ाना चाहिए, न कि उन्हें कमजोर करना चाहिए।

निष्कर्ष

सोर्स कोड विवाद 'डिजिटल संप्रभुता' और 'डिजिटल विश्वास' के बीच के तनाव को दर्शाता है। यद्यपि सरकार की साइबर सुरक्षा में वैध रुचि है, लेकिन अत्यधिक या अपारदर्शी विनियमन भारत की डिजिटल अर्थव्यवस्था को नुकसान पहुंचा सकता है। चुनौती ऐसे स्मार्ट विनियमन बनाने की है जो प्रणालियों को सुरक्षित करे लेकिन उन्हें अधिक जोखिम में न डाले।

मुख्य परीक्षा अभ्यास प्रश्न

प्रश्न 1 (GS III – 15 अंक) स्मार्टफोन सोर्स कोड तक पहुंच की सरकारी मांगों से जुड़ी चिंताओं की चर्चा कीजिए। भारत नवाचार और उपयोगकर्ता के विश्वास के साथ साइबर सुरक्षा की जरूरतों को कैसे संतुलित कर सकता है? (250 शब्द)

प्रश्न 2 (GS II – 10 अंक) भारत में डिजिटल प्रौद्योगिकी नियमों को तैयार करने में पारदर्शिता और हितधारकों के परामर्श के महत्व का परीक्षण कीजिए। (150 शब्द)

प्रश्न 3 (GS IV – नीतिशास्त्र/केस स्टडी) एक सरकारी एजेंसी का तर्क है कि राष्ट्रीय सुरक्षा के लिए सोर्स कोड तक पहुंच आवश्यक है, जबकि कंपनियां और नागरिक समाज गोपनीयता और साइबर सुरक्षा जोखिमों का हवाला देते हैं। एक लोकतांत्रिक राज्य को नैतिक रूप से ऐसे संघर्षों को कैसे हल करना चाहिए?