PLUTUS IAS

CURRENT AFFAIRS

Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

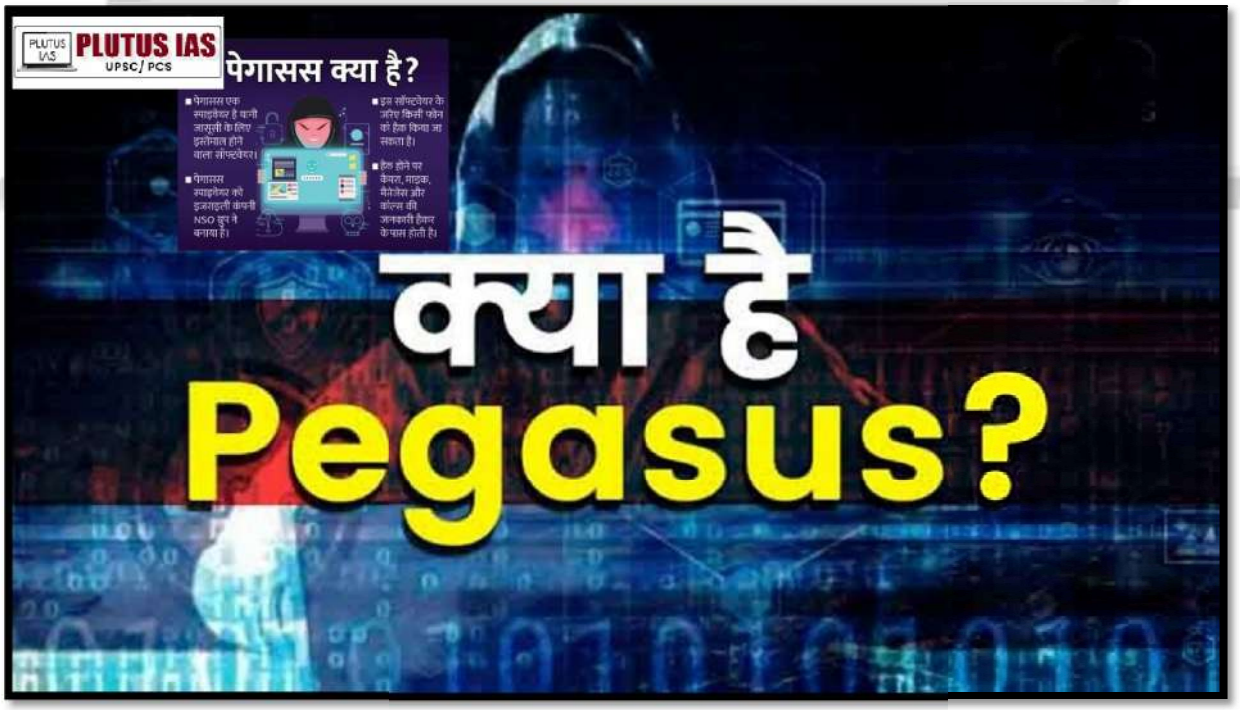
Date –01- January 2025

पेगासस स्पाइवेयर : भारत में राष्ट्रीय एवं साइबर सुरक्षा और निजता के बीच संघर्ष

खबरों में क्यों?

- हाल ही में एक अमेरिकी अदालत ने यह फैसला सुनाया कि पेगासस स्पाइवेयर ने भारत के 300 उपयोगकर्ताओं समेत 1,400 व्हाट्सएप उपयोगकर्ताओं की निगरानी करके कंप्यूटर धोखाधड़ी एवं दुरुपयोग अधिनियम, 1986 का उल्लंघन किया है।
- पेगासस स्पाइवेयर के इस दुरुपयोग ने भारत सहित दुनियाभर में विवाद उत्पन्न किया है, जिसके कारण निजता और मौलिक अधिकारों को लेकर गंभीर चिंताएँ पैदा हुई हैं।

पेगासस स्पाइवेयर क्या है?



- पेगासस स्पाइवेयर को NSO ग्रुप (जो एक इज़रायली साइबर सुरक्षा कंपनी है) द्वारा **विकसित** किया गया है।
- यह स्पाइवेयर iOS और एंड्रॉइड **डिवाइसों** को हैक करके उन पर निगरानी रखने, बातचीत रिकॉर्ड करने, फोटो लेने और ऐप डेटा तक पहुँचने की क्षमता रखता है।
- स्पाइवेयर एक प्रकार का खतरनाक सॉफ़्टवेयर होता है, जो उपयोगकर्ता की अनुमति के बिना डिवाइस पर गुप्त रूप से निगरानी रखता है और जानकारी **एकत्र** करता है।

पेगासस स्पाइवेयर की मुख्य विशेषताएँ :

1. **उन्नत उपयोग :** पेगासस iOS **डिवाइसों** को दूर से जेलब्रेक करने के लिए "ज़ीरो-डे **वल्नरेबिलिटी**" का इस्तेमाल करता है, जबकि एंड्रॉइड डिवाइसों की **निगरानी** के लिए "फ्रामारूट" जैसे सॉफ़्टवेयर का उपयोग किया जाता है।
2. **जीरो-डे वल्नरेबिलिटी :** यह एक **सुरक्षा** खामी है, जिसके लिए कोई सुरक्षा उपाय या पैच उपलब्ध नहीं होता।
3. **रूटिंग :** यह प्रक्रिया किसी डिवाइस को अनलॉक या जेलब्रेक करने की होती है ताकि उस पर पूरा नियंत्रण मिल सके।
4. **इनविजिबिलिटी :** पेगासस का काम गोपनीय होता है और उपयोगकर्ता को इसका कोई स्पष्ट संकेत नहीं मिलता, जैसे कि फिशिंग लिंक पर क्लिक करने के बाद ब्राउज़र बंद होने के अलावा कुछ नहीं **दिखता**।
5. **पेगासस क्लाइंट और संबंधित विवाद :** NSO ग्रुप का कहना है कि पेगासस का उपयोग केवल सरकारों द्वारा किया जाता है। यह विवादास्पद इसलिए है क्योंकि इसका उपयोग आतंकवाद और अपराध को रोकने के बदले, कोई भी सरकार इसका इस्तेमाल पत्रकारों, **विपक्षी** नेताओं, कार्यकर्ताओं और अपने आलोचकों की जासूसी के लिए भी कर सकती हैं।

भारत में पेगासस का उपयोग किस प्रकार किया गया ?

1. **पेगासस परियोजना :** एक वैश्विक जांच में यह खुलासा हुआ कि इज़रायली NSO समूह द्वारा विकसित पेगासस स्पाइवेयर का उपयोग करके 300 से अधिक भारतीय मोबाइल नंबरों को निशाना बनाया गया। इन नंबरों में मंत्रियों, विपक्षी नेताओं, पत्रकारों, वकीलों, व्यापारियों, वैज्ञानिकों, मानवाधिकार कार्यकर्ताओं और सरकारी अधिकारियों के शामिल होने की जानकारी मिली।
2. **एमनेस्टी इंटरनेशनल रिसर्च :** एमनेस्टी इंटरनेशनल की सिक्योरिटी लैब ने पुष्टि की कि पेगासस का उपयोग 37 फोन को हैक करने के लिए किया गया, जिनमें से 10 फोन भारतीय थे।
3. **भीमा कोरेगाँव मामला :** वर्ष 2019 में पेगासस का उपयोग कथित रूप से भीमा कोरेगाँव मामले और महाराष्ट्र तथा छत्तीसगढ़ में दलित अधिकार आंदोलनों से जुड़े वकीलों और कार्यकर्ताओं के खिलाफ किया गया था।
4. **केंद्र सरकार द्वारा RTI आवेदन के जवाब में प्रतिक्रिया :** केंद्र सरकार ने 2013 में एक RTI आवेदन के जवाब में यह बताया कि हर महीने 7,500 से 9,000 टेलीफोन इंटरसेप्शन वारंट जारी होते हैं। हालांकि अब, ऐसी जानकारी के लिए RTI आवेदन राष्ट्रीय सुरक्षा और व्यक्तियों की शारीरिक सुरक्षा को खतरा बताते हुए अस्वीकार कर दिए जाते हैं।
5. **सोशल मीडिया व्हाट्सएप का आरोप :** व्हाट्सएप ने आरोप लगाया कि अप्रैल 2018 से मई 2020 के बीच, NSO समूह ने अपने सोर्स कोड को रिवर्स-इंजीनियरिंग और डीकंपाइल करके "हेवन (Heaven)", "ईडन (Eden)" और "इराइज्ड (Erised)" जैसे इंस्टॉलेशन वैक्टर विकसित किए थे। ये सभी "हमिंगबर्ड (Hummingbird)" नामक एक हैकिंग सूट का हिस्सा थे, जिसे NSO समूह ने अपने सरकारी ग्राहकों को बेचा था।

भारत में निगरानी और डेटा संरक्षण के लिए मौजूद वर्तमान कानूनी ढाँचा :

1. **दूरसंचार अधिनियम, 2023 :** इस अधिनियम की धारा 20(2) के अनुसार, केंद्र या राज्य सरकारों को सार्वजनिक आपात स्थितियों, आपदाओं या सुरक्षा के दौरान दूरसंचार सेवाओं और नेटवर्क का अस्थायी नियंत्रण लेने का अधिकार मिलता है। हालांकि, भारतीय टेलीग्राफ नियम, 2007 के तहत संचार अवरोधन के लिए सरकारी प्राधिकरण की मंजूरी आवश्यक है।
2. **सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 :** इस अधिनियम की धारा 69 और इंटरसेप्शन नियम, 2009 के तहत सरकार को कंप्यूटर संसाधनों के माध्यम से किसी भी सूचना की निगरानी, अवरोधन या डिक्रिप्शन करने का अधिकार प्राप्त है।
3. **डिजिटल व्यक्तिगत डेटा संरक्षण (DPDP) अधिनियम, 2023 :** यह अधिनियम भारत में डेटा संरक्षण से संबंधित एक व्यापक गोपनीयता और डेटा संरक्षण कानून है, जो उपयोगकर्ता से सहमति, उसके वैध उपयोग से संबंधित , उल्लंघन, डेटा ट्रस्टी और संसाधक जिम्मेदारी से संबंधित प्रावधानों के माध्यम से व्यक्तियों के डेटा अधिकारों की रक्षा करता है।

भारत में निगरानी से संबंधित चुनौतियाँ :

1. **निजता के अधिकार जैसे मौलिक अधिकारों का उल्लंघन होना :** निगरानी निजता के अधिकार (अनुच्छेद 21) का उल्लंघन करती है, जैसा कि के.एस. पुट्टस्वामी मामले (2017) में चर्चा की गई। इसके अतिरिक्त, नागरिकों की गतिविधियों पर निगरानी रखना संविधान के अनुच्छेद 19(1)(A) के तहत अभिव्यक्ति की स्वतंत्रता पर प्रतिकूल प्रभाव डालता है।

2. **संसदीय या न्यायिक नियंत्रण नहीं होने के कारण पारदर्शिता का अभाव होना :** निगरानी की प्रक्रिया अक्सर गुप्त रूप से की जाती है, क्योंकि संसदीय या न्यायिक नियंत्रण नहीं होता। इससे कार्यपालिका की शक्ति असंगत रूप से बढ़ जाती है, जो संविधान के शक्तियों के पृथक्करण के सिद्धांत को कमजोर करती है।
3. **नागरिकों को अपने अधिकारों की रक्षा के लिए उपाय तलाशने के अधिकारों का उल्लंघन होना :** इसके तहत निगरानी से प्रभावित व्यक्ति अक्सर न्यायालय में अपनी शिकायत दर्ज नहीं कर पाते, क्योंकि उन्हें अपनी निगरानी के बारे में जानकारी नहीं होती। इससे अनुच्छेद 32 और 226 का उल्लंघन होता है, जो नागरिकों को अपने अधिकारों की रक्षा के लिए उपाय तलाशने का अधिकार देता है।
4. **सुरक्षा उपायों की कमी और कार्यपालिका का अतिक्रमण करना :** इससे संवैधानिक पदाधिकारियों, जैसे सर्वोच्च न्यायालय के न्यायाधीशों की निगरानी के मामले में, कार्यपालिका का अतिक्रमण और सुरक्षा उपायों की कमी सामने आई है।
5. **असहमत होने और स्वतंत्र अभिव्यक्ति का दमन करना :** यह निगरानी के डर से खुली चर्चा, रचनात्मकता और असहमति पर रोक लगाता है, जबकि खुली चर्चा, रचनात्मकता और असहमति एक जीवंत लोकतंत्र के लिए अत्यंत आवश्यक हैं।

समाधान / आगे की राह :

- **संतुलित और संवैधानिक अधिकारों के तहत न्यायिक निगरानी की आवश्यकता :** भारत में पेगासस जैसे स्पाइवेयर के दुरुपयोग को रोकने के लिए निगरानी गतिविधियों की न्यायिक निगरानी शुरू करना अत्यंत आवश्यक है। न्यायालयों को यह अधिकार मिलना चाहिए कि वे यह सुनिश्चित करें कि निगरानी आवश्यक, संतुलित और संवैधानिक अधिकारों के अनुरूप हो।
- **उचित आनुपातिकता परीक्षण को लागू करने की आवश्यकता :** साइबर सुरक्षा के तहत एक उचित आनुपातिकता परीक्षण लागू किया जाना चाहिए, ताकि यह सुनिश्चित किया जा सके कि निगरानी का उपयोग केवल तब किया जाए जब यह अत्यंत आवश्यक हो और कम आक्रामक विकल्प समाप्त हो जाएं।
- **साइबर सुरक्षा और पेगासस जैसे स्पाइवेयर के निर्यात के दुरुपयोग को रोकने के लिए सख्त दिशा-निर्देशों की अत्यंत आवश्यकता :** वैश्विक स्तर पर साइबर सुरक्षा और पेगासस जैसे स्पाइवेयर के निर्यात के दुरुपयोग को रोकने के लिए सख्त दिशा-निर्देशों की आवश्यकता है। उपयोगकर्ताओं के डेटा की अनधिकृत निगरानी से सुरक्षा के लिए एंड-टू-एंड एन्क्रिप्शन और अन्य सुरक्षा प्रोटोकॉल को प्राथमिकता दी जानी चाहिए।

स्रोत – इंडियन एक्सप्रे

प्रारंभिक परीक्षा के लिए अभ्यास प्रश्न :

Q.1. पेगासस स्पाइवेयर के संबंध में निम्नलिखित कथनों पर विचार कीजिए :

1. यह iOS और एंड्रॉइड डिवाइसों को हैक करके उनका डेटा एकत्र करता है।
2. यह किसी डिवाइस को रूट या जेलब्रेक करने की प्रक्रिया का हिस्सा नहीं होता।
3. इसका उपयोग केवल सरकारों द्वारा आतंकवाद और अपराध को रोकने के लिए किया जाता है।
4. इसका कार्य गोपनीय होता है, और उपयोगकर्ता को इसका कोई संकेत नहीं मिलता है।

उपर्युक्त कथनों में से पेगासस स्पाइवेयर की मुख्य विशेषताएँ क्या हैं?

A. केवल 1 और 4

B. केवल 2 और 4

C. केवल 1 और 3

D. केवल 2 और 3

उत्तर – A

मुख्य परीक्षा के लिए अभ्यास प्रश्न :

Q.1. भारतीय टेलीग्राफ अधिनियम 1885, सूचना प्रौद्योगिकी अधिनियम 2000 और डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम 2023 की भूमिका के संदर्भ में, पेगासस स्पाइवेयर के दुरुपयोग से उत्पन्न निजता, सुरक्षा और मौलिक अधिकारों की चिंताओं को ध्यान में रखते हुए, चर्चा कीजिए कि भारत में साइबर सुरक्षा, राष्ट्रीय सुरक्षा और नागरिकों के व्यक्तिगत अधिकारों के बीच संतुलन बनाए रखने के लिए किन कदमों की आवश्यकता है?

(शब्द सीमा – 250 अंक – 15)

Dr. Akhilesh Kumar Shrivastava