



भारत में निगरानी से संबंधित कानून व निजता का अधिकार

sanskritiias.com/hindi/news-articles/surveillance-laws-and-right-to-privacy-in-india



(प्रारंभिक परीक्षा : भारतीय राज्यतंत्र और शासन- अधिकारों से संबंधित मुद्दे इत्यादि, राष्ट्रीय और अंतर्राष्ट्रीय महत्त्व की सामयिक घटनाएँ)

(मुख्य परीक्षा, प्रश्नपत्र 2&3 :संघ एवं राज्यों के कार्य तथा उत्तरदायित्व और संचार नेटवर्क के माध्यम से आंतरिक सुरक्षा को चुनौती)

संदर्भ

भारत में लगभग 300 व्यक्तियों को लक्षित कर इज़रायली स्पाइवेयर 'पेगासस' द्वारा जासूसी के मामले में सरकार ने दावा किया है कि भारत में सभी निगरानी प्रणाली प्रक्रियाएँ कानूनी रूप से वैध हैं।

निगरानी से संबंधित कानून

- भारत में संचार निगरानी मुख्य रूप से दो कानूनों के तहत होती है- टेलीग्राफ अधिनियम, 1885 तथा सूचना प्रौद्योगिकी अधिनियम, 2000.
- टेलीग्राफ अधिनियम कॉल के अवरोधन (Interception of Calls) से संबंधित है। वर्ष 1996 में उच्चतम न्यायालय के हस्तक्षेप के पश्चात् सभी प्रकार के इलेक्ट्रॉनिक संचार की निगरानी के लिये आई.टी. अधिनियम को अधिनियमित किया गया था।
- निगरानी के मौजूदा ढाँचे में कमियों को दूर करने के लिये एक व्यापक डेटा संरक्षण कानून अभी तक अधिनियमित नहीं किया गया है।

टेलीग्राफ अधिनियम, 1885

टेलीग्राफ अधिनियम की धारा 5(2) के अनुसार-

1. **कॉल अवरोधन:** सरकार केवल कुछ स्थितियों में ही कॉल को इंटरसेप्ट कर सकती है।

2. भारत की संप्रभुता और अखंडता, राज्य की सुरक्षा, विदेशी राज्यों के साथ मैत्रीपूर्ण संबंध या सार्वजनिक व्यवस्था या किसी अपराध को रोकने के लिये प्रावधान शामिल हैं।
3. **अभिव्यक्ति की स्वतंत्रता पर प्रतिबंध:** संविधान के अनुच्छेद 19(2) के तहत अभिव्यक्ति की स्वतंत्रता पर प्रतिबंध लगाए गए हैं।
4. **सार्वजनिक सुरक्षा:** ये प्रतिबंध किसी सार्वजनिक आपातकाल की घटना या सार्वजनिक सुरक्षा के हित में भी लगाए जा सकते हैं।
5. **पत्रकारों को सुरक्षा:** धारा 5(2) में एक प्रावधान में कहा गया है कि यह वैध अवरोधन पत्रकारों के खिलाफ नहीं किया जा सकता है।

टेलीग्राफ अधिनियम के संबंध में न्यायिक निर्णय

- 'पब्लिक यूनियन फॉर सिविल लिबर्टीज़ बनाम भारत संघ वाद, 1996' में उच्चतम न्यायालय ने टेलीग्राफ अधिनियम के प्रावधानों में प्रक्रियात्मक सुरक्षा उपायों की कमी की ओर इशारा किया तथा अवरोधन के लिये कुछ दिशानिर्देश निर्धारित किये थे।
- न्यायालय ने कहा कि अवरोधन में शामिल अधिकारी पर्याप्त रिकॉर्ड नहीं रख रहे थे।
- न्यायालय ने जारी दिशा-निर्देशों से संबंधित एक समीक्षा समिति का गठन करने का निर्देश दिया, जो टेलीग्राफ अधिनियम की धारा 5(2) के तहत किये गए प्राधिकारों को देख सकती है।
- न्यायालय ने कहा कि टैपिंग किसी व्यक्ति की निजता का गंभीर आक्रमण है।
- अत्यधिक परिष्कृत संचार प्रौद्योगिकी के विकास के साथ, बिना किसी हस्तक्षेप के किसी के घर या कार्यालय की गोपनीयता में बेची गई टेलीफोन बातचीत का अधिकार अतिसंवेदनशील होता जा रहा है।
- न्यायालय ने यह भी कहा कि इसमें कोई संदेह नहीं है कि प्रत्येक सरकार, चाहे वह कितनी भी लोकतांत्रिक हो, अपने खुफिया संगठन द्वारा कुछ हद तक निगरानी अवश्य करती है, लेकिन उसे नागरिकों के निजता के अधिकार को अधिकारियों द्वारा दुरुपयोग से बचाना भी चाहिये।
- उच्चतम न्यायालय के दिशा-निर्देशों ने 2007 में टेलीग्राफ नियमों और बाद में 2009 में आई.टी. अधिनियम के तहत निर्धारित नियमों के आधार नियम 419A को पेश करने का आधार बनाया।

टेलीग्राफ अधिनियम का नियम 419A

- नियम 419A में कहा गया है कि गृह मंत्रालय का एक सचिव केंद्र के मामले में अवरोधन के आदेश पारित कर सकता है।
- राज्यों के मामलों में एक सचिव स्तर का अधिकारी, जो गृह विभाग का प्रभारी होता है, ऐसे निर्देश जारी कर सकता है।
- अपरिहार्य परिस्थितियों में नियम 419A जोड़ता है, ऐसे आदेश एक अधिकारी द्वारा किये जा सकते हैं, जो संयुक्त सचिव के पद से नीचे न हो, जिसे केंद्रीय गृह सचिव या राज्य के गृह सचिव द्वारा विधिवत अधिकृत किया गया है।

सूचना प्रौद्योगिकी अधिनियम, 2000

- सूचना प्रौद्योगिकी अधिनियम की धारा 69 और सूचना प्रौद्योगिकी (सूचना के अवरोधन, निगरानी और डिफ़िंशन के लिये सुरक्षा उपायों की प्रक्रिया) नियम, 2009 को इलेक्ट्रॉनिक निगरानी के कानूनी ढाँचे को आगे बढ़ाने के लिये अधिनियमित किया गया था।
- आई.टी. अधिनियम के तहत डाटा के सभी इलेक्ट्रॉनिक ट्रांसमिशन को इंटरसेप्ट किया जा सकता है।
- अतः पेगासस जैसे स्पाइवेयर को कानूनी रूप से इस्तेमाल करने के लिये सरकार को आई.टी. और टेलीग्राफ अधिनियम दोनों का प्रयोग करना होगा।

- टेलीग्राफ अधिनियम की धारा 5(2) और संविधान के अनुच्छेद 19(2) में उल्लिखित प्रतिबंधों के अतिरिक्त, आई.टी. अधिनियम की धारा 69 एक और पहलू को जोड़ती है, जो इसे और व्यापक बनाती है - जाँच के लिये डिजिटल जानकारी का अवरोधन, निगरानी तथा डिक्विशन।
- यह टेलीग्राफ अधिनियम के तहत निर्धारित शर्त के साथ छूट देता है, जिसके लिये सार्वजनिक सुरक्षा के हित में सार्वजनिक आपातकाल की घटना की आवश्यकता होती है, जो कानून के तहत शक्तियों के दायरे को विस्तृत करती है।

निजता का अधिकार और न्यायिक निर्णय

- उच्चतम न्यायालय ने अगस्त 2017 में जस्टिस के.एस. पुट्टस्वामी (सेवानिवृत्त) और अन्य बनाम भारत संघ वाद के एक ऐतिहासिक निर्णय में सर्वसम्मति से संविधान के अनुच्छेद 14, 19 और 21 के तहत 'निजता के अधिकार' को एक मौलिक अधिकार के रूप में मान्यता प्रदान की थी।
- यह एक 'बिल्डिंग ब्लॉक और कानूनी लड़ाई' का महत्वपूर्ण घटक है, जो राज्य की निगरानी करने की क्षमता को चुनौती प्रस्तुत करता है।
- लेकिन राज्य की आवश्यकताओं तथा निजता व सुरक्षा के मध्य एक 'ग्रे क्षेत्र' बना हुआ है।
- उसी वर्ष, सरकार ने सेवानिवृत्त न्यायमूर्ति बी.एन. श्री कृष्ण की अध्यक्षता में डाटा संरक्षण समिति का गठन किया था।
- इसने पूरे भारत में सार्वजनिक सुनवाई की और वर्ष 2018 में एक डाटा संरक्षण कानून का मसौदा प्रस्तुत किया, जिसे संसद को अभी अधिनियमित करना है।
- हालाँकि, विशेषज्ञों का कहना है कि मसौदा कानून निगरानी सुधार से पर्याप्त रूप से निपटता नहीं है।

कानूनों में विद्यमान अंतराल की पहचान

वर्ष 2012 में, योजना आयोग तथा दिल्ली उच्च न्यायालय के पूर्व मुख्य न्यायाधीश ए.पी. शाह की अध्यक्षता में निजता के मुद्दों पर विशेषज्ञों के समूह को निजता को प्रभावित करने वाले कानूनों में अंतराल की पहचान करने का काम सौंपा गया था।

निष्कर्ष

निगरानी के लिये किसी व्यक्ति के चयन के आधार और सूचना एकत्र करने की सीमा को लिखित रूप में दर्ज किया जाना चाहिये, क्योंकि मौलिक अधिकारों की आधारशिला के विरुद्ध इन कानूनों की व्यापक पहुँच का न्यायालय में परीक्षण नहीं किया गया है।