भारत का निगरानी तंत्र (Surveillance System) सम्बन्धित अधिनियम एवं चिंताएँ

भारत का निगरानी तंत्र (SURVEILLANCE SYSTEM)

पिछले हफ्ते केंद्र सरकार ने 10 केंद्रीय एजेंसियों को ऑनलाइन संचार और डाटा के अवरोधन, निगरानी और डिक्रिप्ट करने के लिए अधिकृत करने की अधिसूचना जारी की है जिसने संसद् और सिविल समाज में उत्तेजना फैला दी है. वर्तमान समय में जहाँ मोबाइल फोन और ऑनलाइन डिजिटल प्लैटफ़ार्म आम आदमी की मूलभूत आवश्यकता बन गये हैं, वहीँ यह प्रश्न भी खड़ा होता है कि इस ऑनलाइन डाटा की निगरानी करना किस हद तक सही और गलत है, यह देश की सुरक्षा की लिए कितना अनिवार्य है, आम आदमी पर इसका क्या प्रभाव पड़ता है और इसे कैसे तर्कसंगत बनाया जा सकता है आदि.

इन 10 केंद्रीय एजेंसियों को दिये गए ये अधिकार किसी अधिनियम के तहत नहीं बल्कि पहले से ही विद्यमान सूचना प्रौद्योगिकी नियम 2009 के तहत जारी हुए हैं. सरकार के इस कदम ने समय की आवश्यकता के अनुरूप निगरानी तंत्र की महत्ता को उजागर किया है.

वर्तमान निगरानी तंत्र अत्यधिक जटिल और भ्रामक है जो दो अधिनियमों से संचालित होता है –

- भारतीय टेलीग्राफ अधिनियम, 1885
- सूचना प्रौद्योगिकी अधिनियम, 2000

1. भारतीय टेलीग्राफ अधिनियम, 1885 के तहत टेलीफोन निगरानी स्वीकृत है.
2. सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत इलेक्ट्रॉनिक निगरानी अधिकृत है
3. प्रक्रियात्मक संरचना दोनों ही अधिनियमों और उनके अंतर्गत बनाये गये नियमों के तहत समान है और वह 1997 के उच्चतम न्यायालय के एक आदेश के तहत संचालित होती है जिसमें यह कहा गया है कि निगरानी अनुरोधों को एक वैसे अधिकारी द्वारा हस्ताक्षरित किया जाना चाहिए जो कम से कम संयुक्त सचिव के स्तर का हो.

वर्तमान व्यवस्था की तीन विशेषताएँ हैं :-

1. निगरानी के बारे में निर्णय कार्यकारी शाखा (समीक्षा-प्रक्रिया सहित) द्वारा लिया जाता है, जिसमें कोई संसदीय या न्यायिक पर्यवेक्षण नहीं होता है.
2. निगरानी व्यवस्था अस्पष्ट और अनेकार्थक है जिसको संविधान के अनुछेद 19(2) से प्रत्यक्ष **उठकर** यहाँ कॉपी पेस्ट कर दिया गया है, जैसे – निगरानी के आधार के रूप में "विदेशी राज्यों के साथ मैत्रीपूर्ण संबंध या भारत की संप्रभुता और अखंडता".
3. निगरानी व्यवस्था अपारदर्शी है क्योंकि यह नहीं बताती कि निर्णय कैसे लिए जाते हैं और उनके ऊपर कानूनी मानक कैसे लागू किए जाते हैं.

निगरानी के लाभ

1. देश की सुरक्षा , संप्रभुता और अखंडता को सुनिश्चित होना
2. आतंकवादी गतिविधियो को समय रहते पता लगाना और आंतकवादी घटनाओं में कमी
3. दंगो, षडयंत्रो और राष्ट्रद्रोहों जैसी आंतरिक घटनाओं में कमी

4. देश के युवाओं को ISIS जैसे आंतकवादी गुटों से बचाव
5. भ्रष्टाचार पर लगाम
6. डिजिटल मीडिया का प्रयोग करते हुए ब्लैकमेल जैसी घटनाओं में कमी
7. झूठे समाचारों (Fake News) पर लगाम

चिंताएँ

- **निजता के साथ समझौता :-** 2017 में उच्चतम नयायालय ने के.एस. पुट्टास्वामी बनाम भारत संघ मामले में यह निर्णय दिया है की निजता का अधिकार मूल अधिकार है और उस की अवहेलना के लिए कुछ उपयुक्त और वैध कारण होने चाहिएँ जैसे राष्ट्रीय सुरक्षा। देखना यह है कि राज्य कैसे इनके बीच तालमेल बैठाता है .
- इकट्ठा की गई निगरानी सूचना का चोरी हो जाना या व्यक्तिगत लाभ के लिए दुरूपयोग करना
- एक विविधतापूर्ण तंत्र की अनुपस्थिति के कारण जानबूझकर राजनीतिक लाभ के लिए किसी की निजता का हनन और दुरूपयोग
- डिजिटल मीडिया प्लेटफार्म जहाँ एँड-टु-एँड डाटा एँक्रीप्ट होता है उसको डिक्रिप्ट करने के लिए सेवा प्रदाता संस्थानो के साथ काम करना और उनको इसके लिए राजी करना
- प्रशासनिक बोझ में वृद्धि की सम्भावना जबकि कुछ प्रशासनिक संस्थान पहले से ही मानव संसाधनों की कमी से जूझ रहे हैं.

निष्कर्ष

वर्तमान समय में इंटरनेट, मोबाइल और डिजिटल सोशल प्लैटफ़ार्म के कारण किसी सूचना को दुनिया के एक कोने से दूसरे कोने में जाने में समय नहीं लगता और इसके फलस्वरूप मानव जीवन अधिक सुविधापूर्ण हो गया है. लेकिन साथ ही साथ कुछ लोग इनके माध्यम से आंतकवादी गतिविधियाँ, दंगे , झूठे समाचार , भीड़तंत्र, आंदोलन और देश की सुरक्षा से संबन्धित कारोबार चला रहे हैं. वे खुले आम सोशल मीडिया और मोबाइल फोन का प्रयोग करते हुए अपने घृणित उद्देश्यों को अंजाम तक पहुँचाने के लिए प्रयासरत रहत हैं. ऐसी दशा में एक सुदृढ़ निगरानी तंत्र की अनिवार्यता का महत्त्व बढ़ जाता है. अत: एक ऐसे उपयुक्त और लक्षित निगरानी तंत्र की आवश्यकता है जो सोशल मीडिया के दुरूपयोग को कम करे और देश की अर्थव्यवस्था, समाज, शांति, सुरक्षा और संप्रभुता की रक्षा में योगदान करे.

दस सुरक्षा एवं गुप्त सूचना एजेंसियाँ

संदर्भ

हाल ही में भारत सरकार के गृह मंत्रालय ने एक आदेश निर्गत किया है जिसके द्वारा देश की **दस सुरक्षा एवं गुप्त सूचना एजेंसियों** को यह अधिकार दिया गया है कि वे अनुश्रवण करने, कोड तोड़ने और हस्तक्षेप करने के उद्देश्य से किसी भी कंप्यूटर में जमा सूचना तक पहुँच सकते हैं.

ये एजेंसियाँ कौन हैं?

ये दस एजेंसियाँ हैं – गुप्त-सूचना ब्यूरो, नारकोटिक्स कंट्रोल ब्यूरो, प्रवर्तन निदेशालय, केंद्रीय प्रत्यक्ष कर बोर्ड, राजस्व गुप्त-सूचना निदेशालय; केंद्रीय जांच ब्यूरो, राष्ट्रीय जांच एजेंसी कैबिनेट सचिवालय (RAW), गुप्त सूचना निदेशालय (केवल जम्मू-कश्मीर, पूर्वोत्तर एवं असम के सेवा क्षेत्रों के लिए) तथा पुलिस आयुक्त, दिल्ली.

आदेश के मुख्य तथ्य

- सरकार ने इन एजेंसियों को कंप्यूटर में जमा सूचना प्राप्त करने का अधिकार दो अधिनियम/नियम के अनुसार दिया है. ये हैं – सूचना प्रौद्योगिकी अधिनियम, 2000 के **अनुभाग 69/Section 69** तथा सूचना प्रौद्योगिकी प्रक्रिया एवं सुरक्षा नियम, 2009 का नियम 4.
- इस आदेश में यह प्रावधान किया गया है कि किसी भी ग्राहक अथवा सेवा प्रदाता अथवा कंप्यूटर संसाधन के प्रभार में किसी भी व्यक्ति को इन एजेंसियों को तकनीकी सहायता उपलब्ध करानी होगी.
- आदेश का अनुपालन नहीं करने पर सम्बंधित व्यक्ति को सात वर्ष की कैद और जुर्माना होगा.

व्यक्त की जा रहीं चिंताएँ

पहले ऐसा होता था कि केवल गतिशील डाटा को ही सरकार जाँच सकती थी किन्तु अब पुनर्जीवित, भंडारित एवं उत्पादित डाटा भी सरकार इन एजेंसियों के माध्यम से देख सकती है क्योंकि इन्हें जब्ती की कार्रवाई करने की भी शक्ति दी गई है. इसका अर्थ यह हुआ कि न केवल बातचीत अथवा ई-मेल अपितु कंप्यूटर में पाया गया कोई भी डाटा, एजेंसियों को उपलब्ध कराना होगा. एजेंसियों को कंप्यूटर आदि को जब्त करने का भी अधिकार होगा. इस प्रकार बिना किसी रोक-टोक के इन एजेंसियों को फ़ोन की बात-चीत और कंप्यूटर के अंदर झाँकने की अथाह शक्ति दे दी है जो बड़ी चिंता की बात है. हो सकता है कि इस शक्ति का दुरूपयोग भी हो.