INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (online)
ISSN 2348 - 9359 (Print)

An Internationally Indexed Peer Reviewed & Refereed Journal

www.IRJMSH.com
www.isarasolutions.com

Published by iSaRa Solutions

डिजिटल राज्य में निगरानी और निजता का संतुलन: भारत का एक मानक (Normative) विश्लेषण

Suneeta

Research Scholar

सार (Abstract)

यह शोध-पत्र आधुनिक डिजिटल शासन के तीव्र विस्तार के संदर्भ में निगरानी (surveillance) और निजता (privacy) के बीच उत्पन्न होने वाले जटिल तनाव का गहन विश्लेषण प्रस्तुत करता है। सूचना एवं संचार प्रौद्योगिकी (ICT) के विकास ने राज्य की कार्यप्रणाली को अधिक डेटा-आधारित, केंद्रीकृत और दक्ष बनाया है, जिसके परिणामस्वरूप शासन की क्षमता (state capacity) में उल्लेखनीय वृद्धि हुई है। भारतीय परिप्रेक्ष्य में, Aadhaar और Digital India जैसी प्रमुख पहलों ने प्रशासनिक दक्षता, सेवा वितरण, वित्तीय समावेशन और पारदर्शिता को सुदृढ़ किया है। हालाँकि, इन तकनीकी प्रगतियों के साथ-साथ नागरिकों के मौलिक अधिकारों–विशेषकर निजता, अभिव्यक्ति की स्वतंत्रता और व्यक्तिगत स्वायत्तता–पर गंभीर प्रश्न भी उभरकर सामने आए हैं। यह शोध-पत्र इस बात का विश्लेषण करता है कि राज्य की बढ़ती निगरानी क्षमताएँ किस प्रकार नागरिक स्वतंत्रताओं को प्रभावित करती हैं, और क्या ये प्रथाएँ लोकतांत्रिक मूल्यों एवं संवैधानिक सिद्धांतों के अनुरूप हैं।

अध्ययन में एक **मानक (normative) दृष्टिकोण** अपनाया गया है, जिसके अंतर्गत निगरानी की वैधता का परीक्षण पाँच प्रमुख सिद्धांतों–**वैधता (legality), आवश्यकता (necessity), अनुपातिकता (proportionality), पारदर्शिता (transparency) और उत्तरदायित्व (accountability)**–के आधार पर किया गया है। यह ढांचा यह सुनिश्चित करता है कि निगरानी केवल तभी स्वीकार्य हो जब वह स्पष्ट कानूनी आधार पर स्थापित हो, वास्तविक आवश्यकता से प्रेरित हो, अपने उद्देश्य के अनुरूप सीमित हो, पारदर्शी ढंग से संचालित हो तथा उसके लिए प्रभावी जवाबदेही तंत्र उपलब्ध हो।

अध्ययन के निष्कर्ष यह संकेत करते हैं कि भारत की डिजिटल निगरानी व्यवस्था एक द्वैत स्वरूप प्रस्तुत करती है–जहाँ एक ओर यह शासन को अधिक कुशल और प्रभावी बनाती है, वहीं दूसरी ओर यह नागरिकों की निजता और स्वतंत्रता के लिए संभावित खतरा भी उत्पन्न करती है।

विशेष रूप से, व्यापक डेटा संग्रहण, केंद्रीकरण और प्रोफाइलिंग की प्रवृत्तियाँ एक "निगरानी राज्य" (surveillance state) की आशंका को जन्म देती हैं।

अतः, यह शोध-पत्र इस निष्कर्ष पर पहुँचता है कि निगरानी आधुनिक राज्य के लिए पूर्णतः अपरिहार्य हो सकती है, किन्तु इसकी वैधता और औचित्य केवल तभी स्वीकार्य है जब यह **सीमित, नियंत्रित और उत्तरदायी ढांचे** के भीतर संचालित हो। इस प्रकार, एक संतुलित दृष्टिकोण की आवश्यकता है, जिसमें **सुरक्षा और स्वतंत्रता परस्पर पूरक तत्वों** के रूप में कार्य करें और तकनीकी प्रगति मानवाधिकारों के संरक्षण के साथ-साथ शासन की प्रभावशीलता को भी सुनिश्चित करे।

कुंजी शब्द (Keywords):
निगरानी, निजता, डिजिटल शासन, राज्य क्षमता, मानवाधिकार, डेटा संरक्षण, लोकतंत्र

1. प्रस्तावना (Introduction)

डिजिटल युग में शासन की प्रकृति में एक गहरा और संरचनात्मक परिवर्तन देखने को मिला है। सूचना एवं संचार प्रौद्योगिकी (Information and Communication Technology - ICT) के तीव्र विकास ने राज्य की कार्यप्रणाली को अधिक **डेटा-आधारित, केंद्रीकृत और तकनीक-संचालित** बना दिया है। इस परिवर्तन ने न केवल प्रशासनिक दक्षता को बढ़ाया है, बल्कि नीति-निर्माण, सेवा वितरण और संसाधन प्रबंधन के तरीकों को भी पुनर्परिभाषित किया है।

भारत के संदर्भ में, डिजिटल शासन (digital governance) की पहलें–जैसे Aadhaar और Digital India–ने राज्य की क्षमता (state capacity) को उल्लेखनीय रूप से सुदृढ़ किया है। इन पहलों के माध्यम से सरकारी सेवाओं का डिजिटलीकरण, लाभार्थियों की पहचान का सटीक निर्धारण, और सार्वजनिक वितरण प्रणाली में पारदर्शिता सुनिश्चित करने में महत्वपूर्ण प्रगति हुई है। विशेष रूप से, Direct Benefit Transfer (DBT) जैसी व्यवस्थाओं ने मध्यस्थों की भूमिका को कम करते हुए लाभ सीधे नागरिकों तक पहुँचाने में सहायता की है।

हालाँकि, इस तकनीकी प्रगति के साथ-साथ एक गंभीर और जटिल प्रश्न भी उभरकर सामने आया है–**राज्य की बढ़ती निगरानी क्षमता (surveillance capacity)** और नागरिकों की **निजता (privacy) एवं स्वतंत्रता (liberty)** के बीच संतुलन का प्रश्न। डिजिटल तकनीकों के माध्यम से राज्य अब नागरिकों के व्यक्तिगत डेटा, संचार और व्यवहार संबंधी सूचनाओं तक अभूतपूर्व पहुँच प्राप्त कर सकता है। यह स्थिति, यदि उचित नियंत्रण और नियमन के बिना विकसित होती है, तो नागरिकों के मौलिक अधिकारों–विशेषकर निजता के अधिकार–के लिए चुनौती उत्पन्न कर सकती है।

निगरानी के इस विस्तार के कई आयाम हैं–जैसे बायोमेट्रिक पहचान, इंटरनेट और संचार निगरानी, डेटा एनालिटिक्स, और कृत्रिम बुद्धिमत्ता आधारित प्रोफाइलिंग। ये सभी उपकरण शासन को अधिक प्रभावी बनाते हैं, किन्तु साथ ही यह जोखिम भी उत्पन्न करते हैं कि राज्य की शक्ति अत्यधिक केंद्रीकृत और अनियंत्रित हो सकती है। ऐसी स्थिति में "निगरानी राज्य" (surveillance state) की अवधारणा प्रासंगिक हो जाती है, जहाँ नागरिकों की गतिविधियाँ निरंतर अवलोकन के अधीन होती हैं।

इस संदर्भ में, भारतीय संवैधानिक ढाँचे में निजता के अधिकार को विशेष महत्व प्राप्त हुआ है, जिसे Justice K.S. Puttaswamy v. Union of India के ऐतिहासिक निर्णय में मौलिक अधिकार के रूप में मान्यता दी गई। इस निर्णय ने यह स्पष्ट किया कि राज्य की कोई भी निगरानी गतिविधि वैध, आवश्यक और अनुपातिक होनी चाहिए, और यह नागरिकों के अधिकारों के साथ संतुलन बनाए रखे।

अतः, यह शोध-पत्र इसी मूलभूत द्वंद्व–**निगरानी बनाम निजता**–का विश्लेषण करता है। इसका उद्देश्य यह समझना है कि डिजिटल शासन के वर्तमान ढाँचे में राज्य की शक्ति और नागरिकों की स्वतंत्रता के बीच संतुलन कैसे स्थापित किया जा सकता है। इसके लिए यह अध्ययन एक मानक (normative) दृष्टिकोण अपनाता है, जो निगरानी की वैधता का परीक्षण करने के लिए एक सुसंगत और व्यावहारिक ढाँचा प्रस्तुत करता है।

इस प्रकार, यह प्रस्तावना न केवल अध्ययन के विषय की प्रासंगिकता को स्पष्ट करती है, बल्कि यह भी दर्शाती है कि डिजिटल युग में लोकतांत्रिक मूल्यों की रक्षा के लिए निगरानी और निजता के बीच संतुलन स्थापित करना क्यों अनिवार्य है।

2. सैद्धांतिक आधार (Theoretical Framework)

निगरानी (surveillance) और राज्य शक्ति (state power) के संबंध को समझने के लिए एक सुदृढ़ सैद्धांतिक आधार आवश्यक है, जो इस अध्ययन के विश्लेषण को वैचारिक गहराई प्रदान करता है। इस संदर्भ में आधुनिक सामाजिक और राजनीतिक सिद्धांतकारों के विचार विशेष रूप से महत्वपूर्ण हैं, जिन्होंने शक्ति, नियंत्रण और स्वतंत्रता के बीच संबंधों को स्पष्ट किया है।

सबसे पहले, Michel Foucault द्वारा प्रतिपादित "Panopticon" सिद्धांत निगरानी की आधुनिक अवधारणा को समझने के लिए एक केंद्रीय ढांचा प्रदान करता है। फूको ने अपनी प्रसिद्ध कृति *Discipline and Punish* में जेरेमी बेंथम के Panopticon मॉडल का उपयोग करते हुए यह दर्शाया कि आधुनिक समाज में शक्ति का प्रयोग प्रत्यक्ष दमन के बजाय सूक्ष्म और अदृश्य

निगरानी के माध्यम से किया जाता है। Panopticon एक ऐसी संरचना है जिसमें एक केंद्रीय प्रहरी (observer) सभी व्यक्तियों पर नज़र रख सकता है, जबकि व्यक्तियों को यह ज्ञात नहीं होता कि उन्हें कब देखा जा रहा है। इस "दृश्यता की असमानता" (asymmetry of visibility) के कारण व्यक्ति स्वयं को अनुशासित करने लगते हैं।

फूको के अनुसार, आधुनिक राज्य में निगरानी केवल एक प्रशासनिक उपकरण नहीं है, बल्कि यह सामाजिक नियंत्रण का एक प्रभावी माध्यम बन जाती है। यह शक्ति का ऐसा रूप है जो बाहरी बल प्रयोग के बजाय आंतरिक अनुशासन (internal discipline) उत्पन्न करता है। इस दृष्टिकोण से, डिजिटल युग में विकसित निगरानी प्रणालियाँ–जैसे डेटा संग्रहण, बायोमेट्रिक पहचान और एल्गोरिदमिक विश्लेषण–Panopticon की अवधारणा का एक उन्नत और व्यापक रूप प्रस्तुत करती हैं, जहाँ निगरानी निरंतर, सर्वव्यापी और अदृश्य हो जाती है।

दूसरी ओर, निजता (privacy) के सैद्धांतिक आधार को समझने के लिए उदारवादी (liberal) परंपरा के विचारकों का योगदान महत्वपूर्ण है। John Locke ने व्यक्तिगत स्वतंत्रता और प्राकृतिक अधिकारों की अवधारणा को स्थापित करते हुए यह प्रतिपादित किया कि राज्य की शक्ति सीमित होनी चाहिए और व्यक्ति की स्वतंत्रता सर्वोपरि है। इसी प्रकार, John Stuart Mill ने अपनी कृति *On Liberty* में "harm principle" के माध्यम से यह स्पष्ट किया कि राज्य केवल तभी हस्तक्षेप कर सकता है जब किसी व्यक्ति के कार्य से दूसरों को हानि पहुँचती हो।

आधुनिक संदर्भ में, निजता को केवल "अकेले रहने का अधिकार" (right to be let alone) नहीं माना जाता, बल्कि इसे मानव गरिमा (human dignity), स्वायत्तता (autonomy) और आत्म-अभिव्यक्ति (self-expression) का आधार माना जाता है। Daniel J. Solove और Helen Nissenbaum जैसे समकालीन विद्वानों ने निजता को एक बहुआयामी अवधारणा के रूप में विकसित किया है। निसेनबाम की "contextual integrity" की अवधारणा विशेष रूप से यह दर्शाती है कि निजता का उल्लंघन तब होता है जब सूचना का प्रवाह उसके सामाजिक संदर्भ के अनुरूप नहीं होता।

इस प्रकार, निगरानी और निजता के बीच संबंध को एक द्वंद्वात्मक (dialectical) रूप में समझा जा सकता है–जहाँ एक ओर राज्य की शक्ति नियंत्रण और व्यवस्था बनाए रखने के लिए निगरानी का उपयोग करती है, वहीं दूसरी ओर नागरिकों की स्वतंत्रता और गरिमा निजता के संरक्षण की मांग करती है।

अतः, इस अध्ययन में प्रस्तुत सैद्धांतिक आधार यह स्पष्ट करता है कि निगरानी को केवल एक तकनीकी या प्रशासनिक प्रक्रिया के रूप में नहीं देखा जा सकता, बल्कि यह एक व्यापक सामाजिक, राजनीतिक और नैतिक प्रश्न है। इसी कारण, निगरानी की वैधता का मूल्यांकन एक मानक (normative) दृष्टिकोण के माध्यम से किया जाना आवश्यक है, जो यह सुनिश्चित करे कि राज्य की शक्ति लोकतांत्रिक मूल्यों और मानवाधिकारों के अनुरूप सीमित और उत्तरदायी बनी रहे।

3. भारत में डिजिटल निगरानी (Digital Surveillance in India)

भारत में डिजिटल निगरानी (digital surveillance) का विस्तार पिछले दो दशकों में अत्यंत तीव्र गति से हुआ है। सूचना एवं संचार प्रौद्योगिकी (ICT) के विकास, इंटरनेट के व्यापक प्रसार, मोबाइल कनेक्टिविटी में वृद्धि और डिजिटल शासन (e-governance) की पहलों ने राज्य को नागरिकों से संबंधित विशाल मात्रा में डेटा एकत्रित, संग्रहीत और विश्लेषित करने की अभूतपूर्व क्षमता प्रदान की है। इस परिप्रेक्ष्य में, भारत की निगरानी व्यवस्था बहु-स्तरीय (multi-layered) और बहु-आयामी (multi-dimensional) स्वरूप ग्रहण कर चुकी है।

(i) बायोमेट्रिक पहचान प्रणाली (Aadhaar)

भारत में डिजिटल निगरानी के सबसे महत्वपूर्ण स्तंभों में से एक है Aadhaar, जो विश्व की सबसे बड़ी बायोमेट्रिक पहचान प्रणाली मानी जाती है। इस प्रणाली के अंतर्गत नागरिकों की उंगलियों के निशान, आईरिस स्कैन और जनसांख्यिकीय जानकारी को एक केंद्रीकृत डेटाबेस में संग्रहीत किया जाता है।

Aadhaar का प्रमुख उद्देश्य पहचान सत्यापन को सरल बनाना और सरकारी योजनाओं के लक्षित वितरण को सुनिश्चित करना है। इसके माध्यम से Direct Benefit Transfer (DBT), सब्सिडी वितरण और वित्तीय समावेशन जैसे क्षेत्रों में उल्लेखनीय सुधार हुआ है।

किन्तु, इस प्रणाली के साथ कुछ महत्वपूर्ण चिंताएँ भी जुड़ी हुई हैं, जैसे–

- डेटा का अत्यधिक केंद्रीकरण
- संभावित डेटा उल्लंघन (data breaches)
- नागरिकों की गतिविधियों की ट्रैकिंग और प्रोफाइलिंग की संभावना

इस प्रकार, Aadhaar एक ओर शासन को सशक्त बनाता है, वहीं दूसरी ओर यह निगरानी के एक शक्तिशाली उपकरण के रूप में भी उभरता है।

(ii) डिजिटल शासन प्लेटफॉर्म (Digital Governance Platforms)

भारत में Digital India पहल के अंतर्गत विभिन्न डिजिटल प्लेटफॉर्म विकसित किए गए हैं, जिनका उद्देश्य शासन को अधिक पारदर्शी, सुलभ और कुशल बनाना है।

इन प्लेटफॉर्म्स के अंतर्गत शामिल हैं:

- ऑनलाइन सेवा वितरण (e-services)
- डिजिटल भुगतान प्रणाली (UPI, DBT)
- ई-गवर्नेंस पोर्टल्स
- स्वास्थ्य, शिक्षा और वित्तीय सेवाओं के डिजिटल डेटाबेस

इन प्रणालियों ने नागरिकों और राज्य के बीच संवाद को सरल बनाया है तथा सेवाओं की पहुँच को व्यापक किया है। साथ ही, नीति-निर्माण के लिए डेटा-आधारित निर्णय (data-driven governance) को भी प्रोत्साहन मिला है।

हालाँकि, इन प्लेटफॉर्म्स के माध्यम से नागरिकों के व्यक्तिगत और व्यवहारिक डेटा का विशाल संग्रहण होता है, जिससे निम्नलिखित जोखिम उत्पन्न होते हैं:

- विभिन्न डेटाबेस का एकीकरण (data integration)
- नागरिकों की डिजिटल प्रोफाइलिंग
- डेटा के दुरुपयोग की संभावना

(iii) इंटरनेट और संचार निगरानी (Internet and Communication Surveillance)

भारत में इंटरनेट और संचार माध्यमों की निगरानी भी डिजिटल निगरानी व्यवस्था का एक महत्वपूर्ण घटक है। राज्य विभिन्न तकनीकी और कानूनी साधनों के माध्यम से संचार गतिविधियों की निगरानी करता है, जैसे:

- कॉल डेटा रिकॉर्ड (CDR) का विश्लेषण
- इंटरनेट ट्रैफिक मॉनिटरिंग
- सोशल मीडिया गतिविधियों की निगरानी
- ईमेल और डिजिटल संचार का विश्लेषण

इनका उपयोग मुख्यतः राष्ट्रीय सुरक्षा, आतंकवाद-निरोध और अपराध नियंत्रण के उद्देश्यों के लिए किया जाता है।

इसके अतिरिक्त, NATGRID, Central Monitoring System (CMS) और NETRA जैसे कार्यक्रमों के माध्यम से निगरानी क्षमताओं को और अधिक उन्नत किया गया है। ये प्रणालियाँ विभिन्न स्रोतों से डेटा एकत्रित कर उसे एकीकृत रूप में विश्लेषित करने की क्षमता रखती हैं।

(iv) निगरानी के लाभ और जोखिम (Benefits and Risks)

डिजिटल निगरानी के विस्तार से शासन को कई महत्वपूर्ण लाभ प्राप्त हुए हैं:

- प्रशासनिक दक्षता में वृद्धि
- सेवा वितरण में सुधार
- भ्रष्टाचार में कमी
- सुरक्षा तंत्र को सुदृढ़ करना

किन्तु, इसके साथ-साथ कई गंभीर चुनौतियाँ भी उभरकर सामने आई हैं:

- **डेटा केंद्रीकरण (data centralization):** बड़े पैमाने पर डेटा एक ही स्थान पर संग्रहित होने से सुरक्षा जोखिम बढ़ते हैं
- **प्रोफाइलिंग (profiling):** नागरिकों के व्यवहार और गतिविधियों का विश्लेषण कर उनके बारे में विस्तृत प्रोफाइल तैयार किए जा सकते हैं
- **mass surveillance का खतरा:** व्यापक और अनियंत्रित निगरानी नागरिक स्वतंत्रताओं को प्रभावित कर सकती है
- **निजता का उल्लंघन:** व्यक्तिगत डेटा के अनधिकृत उपयोग की संभावना

(v) समग्र विश्लेषण (Overall Analysis)

इस प्रकार, भारत में डिजिटल निगरानी एक **द्वैत (dual) स्वरूप** प्रस्तुत करती है। एक ओर यह शासन को अधिक सक्षम, पारदर्शी और प्रभावी बनाती है, वहीं दूसरी ओर यह नागरिकों की निजता, स्वतंत्रता और मानवाधिकारों के लिए संभावित खतरा भी उत्पन्न करती है।

अतः यह आवश्यक हो जाता है कि डिजिटल निगरानी को एक **नियंत्रित, संतुलित और उत्तरदायी ढांचे** के भीतर संचालित किया जाए, जिससे इसके लाभों को सुरक्षित रखते हुए इसके जोखिमों को न्यूनतम किया जा सके।

4. कानूनी परिप्रेक्ष्य (Legal Perspective)

भारत में डिजिटल निगरानी और निजता के प्रश्न को समझने के लिए एक सुदृढ़ **कानूनी एवं संवैधानिक ढाँचा** अत्यंत आवश्यक है। भारतीय संविधान नागरिकों के मौलिक अधिकारों की रक्षा

करता है, और समय के साथ न्यायपालिका ने इन अधिकारों की व्याख्या करते हुए उन्हें नए सामाजिक एवं तकनीकी संदर्भों के अनुरूप विकसित किया है।

(i) निजता का संवैधानिक आधार (Constitutional Basis of Privacy)

भारतीय संविधान में "निजता" (privacy) का स्पष्ट उल्लेख प्रारंभिक रूप से नहीं किया गया था, किन्तु न्यायिक व्याख्या के माध्यम से इसे **अनुच्छेद 21 (जीवन और व्यक्तिगत स्वतंत्रता का अधिकार)** के अंतर्गत विकसित किया गया।

इस संदर्भ में, Justice K.S. Puttaswamy v. Union of India का ऐतिहासिक निर्णय एक मील का पत्थर है। इस मामले में भारत के सर्वोच्च न्यायालय की नौ-न्यायाधीशों की पीठ ने सर्वसम्मति से यह घोषित किया कि **निजता का अधिकार (Right to Privacy) एक मौलिक अधिकार है**, जो मानव गरिमा, स्वायत्तता और व्यक्तिगत स्वतंत्रता का अभिन्न अंग है।

न्यायालय ने यह भी स्पष्ट किया कि निजता केवल शारीरिक (physical privacy) तक सीमित नहीं है, बल्कि इसमें **सूचनात्मक निजता (informational privacy)** और **निर्णयात्मक स्वायत्तता (decisional autonomy)** भी शामिल है।

(ii) राज्य हस्तक्षेप की सीमाएँ (Limits on State Intervention)

Puttaswamy निर्णय में न्यायालय ने यह निर्धारित किया कि राज्य द्वारा नागरिकों के अधिकारों में किसी भी प्रकार का हस्तक्षेप एक **तीन-स्तरीय परीक्षण (three-fold test)** के अधीन होगा:

1. **वैधता (Legality):**
   हस्तक्षेप स्पष्ट और विधिवत् स्थापित कानून द्वारा अधिकृत होना चाहिए।
2. **आवश्यकता (Necessity):**
   हस्तक्षेप किसी वैध राज्य उद्देश्य–जैसे राष्ट्रीय सुरक्षा, सार्वजनिक व्यवस्था या अपराध नियंत्रण–के लिए आवश्यक होना चाहिए।
3. **अनुपातिकता (Proportionality):**
   हस्तक्षेप का दायरा और प्रभाव उस उद्देश्य के अनुरूप होना चाहिए, और यह अत्यधिक या अनावश्यक नहीं होना चाहिए।

यह परीक्षण यह सुनिश्चित करता है कि राज्य की शक्ति **मनमानी (arbitrary)** न हो और नागरिकों के अधिकारों की रक्षा बनी रहे।

(iii) पूर्ववर्ती न्यायिक दृष्टिकोण (Earlier Judicial Approach)

Puttaswamy निर्णय से पूर्व, भारतीय न्यायपालिका ने निजता के अधिकार को लेकर मिश्रित दृष्टिकोण अपनाया था।

- Kharak Singh v. State of Uttar Pradesh में न्यायालय ने निजता को स्पष्ट रूप से मौलिक अधिकार के रूप में स्वीकार नहीं किया, किन्तु व्यक्तिगत स्वतंत्रता के कुछ पहलुओं को संरक्षित किया।
- PUCL v. Union of India में टेलीफोन टैपिंग के संदर्भ में न्यायालय ने यह माना कि अनियंत्रित निगरानी नागरिकों के अधिकारों का उल्लंघन कर सकती है, और इसके लिए प्रक्रिया संबंधी सुरक्षा (procedural safeguards) आवश्यक हैं।

इन निर्णयों ने आगे चलकर निजता के अधिकार को एक स्वतंत्र संवैधानिक अधिकार के रूप में मान्यता देने की नींव रखी।

(iv) वैधानिक ढाँचा (Statutory Framework)

भारत में डिजिटल निगरानी और डेटा उपयोग से संबंधित कुछ प्रमुख कानून निम्नलिखित हैं:

- **सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000):**
  यह अधिनियम इलेक्ट्रॉनिक संचार और डेटा से संबंधित अपराधों एवं निगरानी के लिए कानूनी आधार प्रदान करता है।
- **डिजिटल पर्सनल डेटा प्रोटेक्शन अधिनियम, 2023:**
  यह कानून व्यक्तिगत डेटा के संग्रहण, उपयोग और संरक्षण के लिए एक ढांचा प्रदान करता है, जिसका उद्देश्य नागरिकों की सूचनात्मक निजता की रक्षा करना है।
- **टेलीग्राफ अधिनियम, 1885:**
  यह अधिनियम संचार अवरोधन (interception) के लिए कानूनी प्रावधान प्रदान करता है, जिसका उपयोग आज भी विभिन्न संदर्भों में किया जाता है।

हालाँकि, इन कानूनों की प्रभावशीलता और व्यापकता को लेकर अभी भी कई बहसें जारी हैं, विशेषकर डिजिटल युग की जटिलताओं को देखते हुए।

(v) डिजिटल निगरानी और संवैधानिक चुनौतियाँ (Constitutional Challenges)

डिजिटल निगरानी के विस्तार ने कई महत्वपूर्ण संवैधानिक प्रश्न उत्पन्न किए हैं:

- क्या व्यापक डेटा संग्रहण निजता के अधिकार का उल्लंघन करता है?
- क्या निगरानी तंत्र पर्याप्त पारदर्शी और उत्तरदायी हैं?

- क्या नागरिकों के पास अपने डेटा के उपयोग को नियंत्रित करने का अधिकार है?

इन प्रश्नों का समाधान केवल विधायी प्रावधानों से ही नहीं, बल्कि न्यायिक व्याख्या और नीतिगत सुधारों के माध्यम से भी संभव है।

(vi) समग्र विश्लेषण (Overall Analysis)

इस प्रकार, भारत का कानूनी ढाँचा यह स्पष्ट करता है कि निगरानी पूर्णतः प्रतिबंधित नहीं है, बल्कि यह **संवैधानिक सीमाओं के भीतर नियंत्रित** होनी चाहिए। Justice K.S. Puttaswamy v. Union of India का निर्णय इस संतुलन को स्थापित करने का एक मजबूत आधार प्रदान करता है।

अतः, यह कहा जा सकता है कि डिजिटल युग में राज्य की निगरानी शक्तियाँ तभी वैध मानी जाएँगी जब वे **कानूनी, आवश्यक और अनुपातिक** हों, तथा नागरिकों के मौलिक अधिकारों–विशेषकर निजता–का सम्मान करें।

5. निगरानी के प्रभाव (Impact of Surveillance)

डिजिटल युग में निगरानी (surveillance) का प्रभाव बहुआयामी है, जो एक ओर शासन की दक्षता और सुरक्षा को सुदृढ़ करता है, वहीं दूसरी ओर यह नागरिकों की स्वतंत्रता, निजता और सामाजिक समानता के लिए गंभीर चुनौतियाँ भी उत्पन्न करता है। अतः निगरानी के प्रभावों को एक **द्वैत (dual) परिप्रेक्ष्य** में समझना आवश्यक है–सकारात्मक (positive) तथा नकारात्मक (negative) दोनों आयामों में।

(i) सकारात्मक प्रभाव (Positive Impacts)

1. प्रशासनिक दक्षता में वृद्धि (Enhanced Administrative Efficiency)

डिजिटल निगरानी प्रणालियों के माध्यम से राज्य को वास्तविक समय (real-time) में डेटा उपलब्ध होता है, जिससे निर्णय-निर्माण अधिक तेज़ और सटीक हो जाता है।

- सरकारी योजनाओं के कार्यान्वयन की निगरानी आसान होती है
- संसाधनों का बेहतर प्रबंधन संभव होता है
- प्रशासनिक प्रक्रियाओं में देरी और त्रुटियों में कमी आती है

उदाहरण के रूप में, Aadhaar आधारित प्रमाणीकरण प्रणाली ने लाभार्थियों की पहचान को सटीक बनाकर प्रशासनिक कार्यों को अधिक प्रभावी बनाया है।

2. भ्रष्टाचार में कमी (Reduction in Corruption)

निगरानी और डिजिटल ट्रैकिंग के माध्यम से वित्तीय लेन-देन और सरकारी प्रक्रियाओं में पारदर्शिता बढ़ती है।

- Direct Benefit Transfer (DBT) के माध्यम से बिचौलियों की भूमिका कम होती है
- फर्जी लाभार्थियों की पहचान संभव होती है
- सार्वजनिक धन के दुरुपयोग पर नियंत्रण स्थापित होता है

इस प्रकार, डिजिटल निगरानी भ्रष्टाचार को कम करने का एक प्रभावी उपकरण बन सकती है।

3. सेवा वितरण में सुधार (Improved Service Delivery)

डिजिटल प्लेटफॉर्म्स के माध्यम से नागरिकों को सेवाएँ अधिक तेज़, सुलभ और पारदर्शी रूप में प्राप्त होती हैं।

- ऑनलाइन सेवाओं की उपलब्धता
- समय और लागत में कमी
- ग्रामीण एवं दूरस्थ क्षेत्रों तक सेवाओं की पहुँच

Digital India के अंतर्गत विकसित डिजिटल अवसंरचना ने इस दिशा में महत्वपूर्ण योगदान दिया है।

(ii) नकारात्मक प्रभाव (Negative Impacts)

1. निजता का उल्लंघन (Violation of Privacy)

निगरानी का सबसे गंभीर प्रभाव नागरिकों की निजता पर पड़ता है।

- व्यक्तिगत डेटा का व्यापक संग्रहण
- डेटा के दुरुपयोग या लीक होने की संभावना
- नागरिकों की गतिविधियों का निरंतर ट्रैकिंग

यदि इन प्रक्रियाओं पर उचित नियंत्रण न हो, तो यह **सूचनात्मक निजता (informational privacy)** का गंभीर उल्लंघन बन सकता है।

2. "Chilling Effect" (अभिव्यक्ति पर दमनात्मक प्रभाव)

निगरानी के वातावरण में नागरिक यह महसूस कर सकते हैं कि उनकी गतिविधियाँ और विचार लगातार देखे जा रहे हैं।

- लोग अपने विचार खुलकर व्यक्त करने से बचते हैं
- अभिव्यक्ति की स्वतंत्रता सीमित हो जाती है

- लोकतांत्रिक विमर्श (democratic discourse) कमजोर पड़ सकता है

यह "chilling effect" लोकतंत्र के लिए एक गंभीर खतरा है, क्योंकि यह नागरिक सहभागिता को प्रभावित करता है।

3. सामाजिक असमानता (Social Inequality)

निगरानी का प्रभाव समाज के सभी वर्गों पर समान रूप से नहीं पड़ता।

- हाशिए के समूह (marginalized communities) अधिक प्रभावित होते हैं
- डेटा आधारित प्रोफाइलिंग से भेदभाव (discrimination) की संभावना बढ़ती है
- डिजिटल विभाजन (digital divide) के कारण कुछ समूह निगरानी के जोखिमों के प्रति अधिक संवेदनशील हो जाते हैं

इस प्रकार, निगरानी सामाजिक असमानताओं को और गहरा कर सकती है।

(iii) समग्र विश्लेषण (Overall Assessment)

निगरानी के प्रभावों का विश्लेषण यह स्पष्ट करता है कि यह एक **दोहरी प्रकृति (double-edged phenomenon)** है। जहाँ एक ओर यह शासन को अधिक प्रभावी, पारदर्शी और उत्तरदायी बनाती है, वहीं दूसरी ओर यह नागरिकों के मौलिक अधिकारों और लोकतांत्रिक मूल्यों के लिए चुनौती भी प्रस्तुत करती है।

अतः, यह आवश्यक है कि निगरानी के सकारात्मक लाभों को बनाए रखते हुए इसके नकारात्मक प्रभावों को कम करने के लिए एक **संतुलित, नियंत्रित और उत्तरदायी ढांचा** विकसित किया जाए।

6. मानक (Normative) ढांचा

डिजिटल युग में निगरानी (surveillance) की बढ़ती प्रवृत्ति को देखते हुए यह अत्यंत आवश्यक हो जाता है कि इसके उपयोग को एक स्पष्ट, न्यायसंगत और लोकतांत्रिक ढांचे के भीतर नियंत्रित किया जाए। इसी उद्देश्य से इस अध्ययन में एक **मानक (normative) ढांचा** प्रस्तुत किया गया है, जो निगरानी की वैधता और औचित्य का मूल्यांकन करने के लिए पाँच मूलभूत सिद्धांतों पर आधारित है। यह ढांचा न केवल सैद्धांतिक रूप से महत्वपूर्ण है, बल्कि नीति-निर्माण, न्यायिक समीक्षा और प्रशासनिक कार्यप्रणाली के लिए भी एक व्यावहारिक मार्गदर्शक प्रदान करता है।

(i) वैधता (Legality)

वैधता का सिद्धांत यह सुनिश्चित करता है कि किसी भी निगरानी गतिविधि का संचालन **स्पष्ट और विधिवत् स्थापित कानून** के अधीन हो।

- निगरानी केवल उसी स्थिति में वैध मानी जाएगी जब उसे किसी विधि द्वारा अधिकृत किया गया हो
- कानून पारदर्शी, सुसंगत और सार्वजनिक रूप से उपलब्ध होना चाहिए
- मनमानी या गुप्त निगरानी (arbitrary or secret surveillance) को रोका जाना चाहिए

यह सिद्धांत राज्य की शक्तियों को संवैधानिक सीमाओं में बाँधता है और नागरिकों को यह जानकारी देता है कि किन परिस्थितियों में उनकी निगरानी की जा सकती है।

(ii) आवश्यकता (Necessity)

आवश्यकता का सिद्धांत यह निर्धारित करता है कि निगरानी केवल तभी की जानी चाहिए जब वह **वास्तव में अनिवार्य** हो।

- इसका उद्देश्य किसी वैध राज्य हित–जैसे राष्ट्रीय सुरक्षा, सार्वजनिक व्यवस्था या अपराध नियंत्रण–से जुड़ा होना चाहिए
- यदि कोई कम हस्तक्षेपकारी (less intrusive) विकल्प उपलब्ध है, तो उसे प्राथमिकता दी जानी चाहिए

यह सिद्धांत यह सुनिश्चित करता है कि निगरानी "सुविधा" या "प्रशासनिक सरलता" के लिए नहीं, बल्कि वास्तविक आवश्यकता के आधार पर ही लागू की जाए।

(iii) अनुपातिकता (Proportionality)

अनुपातिकता का सिद्धांत निगरानी के **दायरे और प्रभाव** को सीमित करने का कार्य करता है।

- निगरानी का स्तर उसके उद्देश्य के अनुरूप होना चाहिए
- व्यापक (mass) और अंधाधुंध निगरानी से बचा जाना चाहिए
- लाभ और हानि (benefit vs harm) के बीच संतुलन स्थापित होना चाहिए

उदाहरण के लिए, किसी छोटे अपराध की जांच के लिए पूरे समुदाय की निगरानी करना अनुपातिकता के सिद्धांत का उल्लंघन होगा। यह सिद्धांत विशेष रूप से Justice K.S. Puttaswamy v. Union of India के निर्णय में केंद्रीय रूप से लागू किया गया है।

(iv) पारदर्शिता (Transparency)

पारदर्शिता लोकतांत्रिक शासन का एक अनिवार्य तत्व है, जो निगरानी प्रणाली में विश्वास को बनाए रखता है।

- निगरानी से संबंधित नीतियाँ, प्रक्रियाएँ और दिशानिर्देश स्पष्ट होने चाहिए
- सरकार को समय-समय पर **transparency reports** जारी करनी चाहिए

- नागरिकों को यह जानकारी होनी चाहिए कि उनका डेटा कैसे, क्यों और किस उद्देश्य से उपयोग किया जा रहा है

हालाँकि, राष्ट्रीय सुरक्षा जैसे मामलों में पूर्ण पारदर्शिता संभव नहीं हो सकती, फिर भी एक संतुलित स्तर की पारदर्शिता आवश्यक है ताकि लोकतांत्रिक उत्तरदायित्व बना रहे।

(v) उत्तरदायित्व (Accountability)

उत्तरदायित्व का सिद्धांत यह सुनिश्चित करता है कि निगरानी करने वाली एजेंसियाँ अपने कार्यों के लिए **जवाबदेह (answerable)** हों।

- निगरानी गतिविधियों की समीक्षा के लिए स्वतंत्र संस्थाएँ (जैसे न्यायिक या संसदीय निगरानी) होनी चाहिए
- शक्ति के दुरुपयोग की स्थिति में उत्तरदायित्व तय किया जाना चाहिए
- नागरिकों के पास शिकायत और न्याय प्राप्त करने के प्रभावी साधन उपलब्ध होने चाहिए

यह सिद्धांत यह सुनिश्चित करता है कि निगरानी की शक्ति अनियंत्रित न हो और उसके उपयोग पर प्रभावी नियंत्रण बना रहे।

(vi) समग्र दृष्टिकोण (Integrated Framework)

ये पाँचों सिद्धांत–वैधता, आवश्यकता, अनुपातिकता, पारदर्शिता और उत्तरदायित्व–अलग-अलग नहीं, बल्कि एक **एकीकृत (integrated) ढांचे** के रूप में कार्य करते हैं।

☞ **निगरानी तभी वैध और न्यायसंगत मानी जाएगी जब ये पाँचों मानक एक साथ पूरे हों।**

यदि इनमें से कोई एक भी तत्व अनुपस्थित है, तो:

- निगरानी असंवैधानिक या अवैध हो सकती है
- नागरिकों के मौलिक अधिकारों का उल्लंघन हो सकता है
- लोकतांत्रिक संस्थाओं पर विश्वास कमजोर हो सकता है

(vii) भारतीय संदर्भ में प्रासंगिकता (Relevance in Indian Context)

भारत में Aadhaar, Digital India तथा अन्य डिजिटल निगरानी प्रणालियों के संदर्भ में यह मानक ढांचा अत्यंत प्रासंगिक है।

यह नीति-निर्माताओं, न्यायपालिका और प्रशासन के लिए एक मार्गदर्शक सिद्धांत प्रदान करता है, जिससे यह सुनिश्चित किया जा सके कि:

- तकनीकी प्रगति मानवाधिकारों के अनुरूप हो
- राज्य की शक्ति सीमित और उत्तरदायी बनी रहे

- नागरिकों की स्वतंत्रता, निजता और गरिमा संरक्षित रहे

7. निष्कर्ष (Conclusion)

डिजिटल युग में राज्य की कार्यप्रणाली में जो परिवर्तन आया है, उसने शासन को अधिक सक्षम, त्वरित और डेटा-आधारित बना दिया है। सूचना एवं संचार प्रौद्योगिकी (ICT) के विस्तार ने प्रशासनिक दक्षता, सेवा वितरण और राष्ट्रीय सुरक्षा के क्षेत्र में उल्लेखनीय सुधार किए हैं। भारत जैसे विशाल और विविधतापूर्ण लोकतंत्र में, Aadhaar तथा Digital India जैसी पहलों ने शासन को आधुनिक, पारदर्शी और अधिक प्रभावी बनाने में महत्वपूर्ण भूमिका निभाई है।

हालाँकि, इस तकनीकी प्रगति के साथ-साथ एक गंभीर चुनौती भी उभरकर सामने आई है–**निगरानी (surveillance)** और **नागरिक स्वतंत्रता (civil liberties)** के बीच संतुलन की चुनौती। राज्य की बढ़ती निगरानी क्षमताएँ, यदि बिना पर्याप्त कानूनी नियंत्रण, पारदर्शिता और उत्तरदायित्व के प्रयोग की जाती हैं, तो वे नागरिकों के मौलिक अधिकारों–विशेषकर निजता, अभिव्यक्ति की स्वतंत्रता और व्यक्तिगत स्वायत्तता–के लिए खतरा बन सकती हैं।

इस अध्ययन से यह स्पष्ट होता है कि निगरानी का स्वरूप द्वैत (dual) है। एक ओर यह प्रशासनिक दक्षता, भ्रष्टाचार में कमी और सुरक्षा सुनिश्चित करने का एक प्रभावी साधन है, वहीं दूसरी ओर यह mass surveillance, डेटा केंद्रीकरण, प्रोफाइलिंग और "chilling effect" जैसे जोखिमों को जन्म दे सकता है।

भारतीय संवैधानिक परिप्रेक्ष्य में, Justice K.S. Puttaswamy v. Union of India का निर्णय इस संतुलन को स्थापित करने का एक मजबूत आधार प्रदान करता है, जिसमें यह स्पष्ट किया गया है कि राज्य द्वारा किसी भी हस्तक्षेप को **वैध, आवश्यक और अनुपातिक** होना चाहिए।

इसी संदर्भ में, इस शोध-पत्र ने एक **पाँच-सिद्धांत आधारित मानक (normative) ढांचा** प्रस्तुत किया है–

- वैधता
- आवश्यकता
- अनुपातिकता
- पारदर्शिता
- उत्तरदायित्व

यह ढांचा यह सुनिश्चित करता है कि निगरानी केवल तभी न्यायसंगत मानी जाए जब यह लोकतांत्रिक मूल्यों और संवैधानिक सीमाओं के भीतर संचालित हो।

अतः, निष्कर्षतः यह कहा जा सकता है कि:

☞ **निगरानी आधुनिक राज्य के लिए अपरिहार्य हो सकती है, किन्तु इसका उपयोग केवल सीमित, नियंत्रित और उत्तरदायी ढांचे के भीतर ही वैध और न्यायसंगत माना जा सकता है।**

इस संतुलन में ही एक ऐसे लोकतांत्रिक समाज की परिकल्पना निहित है, जहाँ सुरक्षा और स्वतंत्रता परस्पर विरोधी न होकर पूरक (complementary) तत्व के रूप में कार्य करते हैं, और जहाँ तकनीक मानव अधिकारों को सीमित करने के बजाय उन्हें सशक्त बनाने का माध्यम बनती है।

संदर्भ सूची (References)

(A) पुस्तकें (Books)

1. Discipline and Punish - Michel Foucault
2. Two Treatises of Government - John Locke
3. On Liberty - John Stuart Mill
4. Understanding Privacy - Daniel J. Solove
5. Privacy in Context - Helen Nissenbaum
6. Surveillance Studies - David Lyon

(B) न्यायिक निर्णय (Case Laws)

1. Justice K.S. Puttaswamy v. Union of India
2. PUCL v. Union of India
3. Kharak Singh v. State of Uttar Pradesh

(C) कानून एवं नीतियाँ (Laws & Policies)

1. Information Technology Act 2000
2. Digital Personal Data Protection Act 2023
3. Indian Telegraph Act 1885

(D) अंतरराष्ट्रीय दस्तावेज (International Instruments)

1. Universal Declaration of Human Rights
2. International Covenant on Civil and Political Rights
3. General Data Protection Regulation

(E) रिपोर्ट्स एवं अन्य स्रोत (Reports & Others)

1. Internet Freedom Foundation Reports

2. Privacy International Reports
3. Human Rights Watch Reports

भारतीय भाषा, शिक्षा, साहित्य एवं शोध

ISSN 2321 – 9726

WWW.BHARTIYASHODH.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SCIENCE & TECHNOLOGY

ISSN – 2250 – 1959 (0) 2348 – 9367 (P)

WWW.IRJMST.COM

INTERNATIONAL RESEARCH JOURNAL OF COMMERCE, ARTS AND SCIENCE

ISSN 2319 – 9202

WWW.CASIRJ.COM

INTERNATIONAL RESEARCH JOURNAL OF MANAGEMENT SOCIOLOGY & HUMANITIES

ISSN 2277 – 9809 (0) 2348 - 9359 (P)

WWW.IRJMSH.COM

INTERNATIONAL RESEARCH JOURNAL OF SCIENCE ENGINEERING AND TECHNOLOGY

ISSN 2454-3195 (online)

WWW.RJSET.COM

INTEGRATED RESEARCH JOURNAL OF MANAGEMENT, SCIENCE AND INNOVATION

ISSN 2582-5445

WWW.IRJMSI.COM

JOURNAL OF LEGAL STUDIES,POLITICS AND ECONOMICS RESEARCH

WWW.JLPER.COM