ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, January-June 2025, Submitted in April 2025

"भारत में राष्ट्रीय सुरक्षा और निजता का अधिकार: डिजिटल युग में सरकारी निगरानी, संवैधानिक संतुलन और एक नवीन नियामक ढाँचे का अन्वेषण"

डॉ. अभिषेक यादव, पीएचडी, राजनीति विज्ञान विभाग, दीन दयाल उपाध्याय गोरखपुर विश्वविद्यालय, गोरखपुर

शोध सार (Abstract)

भारत जैसे एक संवैधानिक लोकतंत्र में, जहाँ निजता का अधिकार (Right to Privacy) सर्वोच्च न्यायालय के ऐतिहासिक पुट्टुस्वामी निर्णय (Puttaswamy judgment, 2017) द्वारा एक मौलिक अधिकार के रूप में स्थापित किया गया है, राष्ट्रीय सुरक्षा (National Security) के साथ इसका संतुलन बनाना एक जटिल और निरंतर चुनौती है। डिजिटल युग में, सरकारी निगरानी (Government Surveillance) की क्षमताएँ अभूतपूर्व रूप से बढ़ गई हैं, जिनमें कृत्रिम बुद्धिमत्ता (AI), बड़े डेटा विश्लेषण (Big Data Analytics), फेशियल रिकॉग्निशन (Facial Recognition) और साइबर इंटरसेप्शन (Cyber Interception) जैसी प्रौद्योगिकियाँ शामिल हैं। यह शोध पत्र इन उन्नत निगरानी प्रौद्योगिकियों के उदय के मद्देनजर भारत में राष्ट्रीय सुरक्षा के नाम पर व्यक्तिगत स्वतंत्रता पर होने वाले प्रभावों का एक गंभीर मूल्यांकन प्रस्तुत करता है।

यह शोध भारत में मौजूदा कानूनी और संस्थागत ढाँचे (जैसे भारतीय टेलीग्राफ अधिनियम, सूचना प्रौद्योगिकी अधिनियम की धारा 69, आपराधिक प्रक्रिया संहिता) का विश्लेषण करेगा और उनकी अपर्याप्तताओं और पारदर्शिता की कमी को उजागर करेगा, विशेषकर तब जब डिजिटल निगरानी की जटिलताएँ बढ़ती जा रही हैं। पुट्टुस्वामी निर्णय के तहत निर्धारित आनुपातिकता (Proportionality) और आवश्यकता (Necessity) के सिद्धांतों के प्रकाश में, यह शोध भारतीय संदर्भ के लिए एक नवीन नियामक ढाँचे का प्रस्ताव करेगा। इस ढाँचे में कठोर न्यायिक या स्वतंत्र कार्यकारी निरीक्षण, सशक्त संसदीय जवाबदेही, स्पष्ट प्रक्रियात्मक सुरक्षा उपाय, डेटा संरक्षण सिद्धांतों का एकीकरण और सार्वजनिक पारदर्शिता की आवश्यकता पर बल दिया जाएगा। एक तुलनात्मक विश्लेषण के माध्यम से, यह शोध पत्र अन्य लोकतंत्रों (जैसे यूरोपीय संघ, संयुक्त राज्य अमेरिका और यूनाइटेड किंगडम) से सीखे गए सर्वोत्तम अभ्यासों और संभावित चुनौतियों का भी मूल्यांकन करेगा, ताकि भारत के लिए एक यथार्थवादी और संवैधानिक रूप से सुदृढ़ मॉडल विकसित किया जा सके।

यह शोध अंततः भारत में एक ऐसे संतुलित दृष्टिकोण की वकालत करता है जो नागरिक स्वतंत्रता की रक्षा करते हुए वैध राष्ट्रीय सुरक्षा हितों को संबोधित करे, और यह सुनिश्चित करे कि "डिजिटल पैनोप्टिकॉन" (Digital Panopticon) एक संवैधानिक लोकतंत्र के मूल सिद्धांतों को कमजोर न करे।

1: परिचय (Introduction):- यह अध्याय भारत में राष्ट्रीय सुरक्षा और निजता के अधिकार के बीच जटिल और अक्सर तनावपूर्ण संबंधों की पड़ताल करता है, विशेष रूप से डिजिटल युग में सरकारी निगरानी प्रौद्योगिकियों के बढ़ते उपयोग के संदर्भ में। यह शोध समस्या को परिभाषित करेगा, शोध प्रश्नों को प्रस्तुत करेगा, और अध्ययन के दायरे, कार्यप्रणाली और महत्व को रेखांकित करेगा।

1.1. पृष्ठभूमि: निजता और राष्ट्रीय सुरक्षा के बीच द्वंद्व का ऐतिहासिक और संवैधानिक संदर्भ

आधुनिक राज्य के अस्तित्व के साथ ही राष्ट्रीय सुरक्षा की अवधारणा और व्यक्तिगत स्वतंत्रता की रक्षा के बीच एक अंतर्निहित द्वंद्व रहा है। लोकतांत्रिक समाजों में, यह संतुलन नागरिकों को राज्य की मनमानी शक्ति से बचाने के लिए संवैधानिक सिद्धांतों और कानूनी सुरक्षा उपायों के माध्यम से बनाए रखा जाता है। भारत में, यह द्वंद्व विशेष रूप से जटिल रहा है, जिसका एक हिस्सा औपनिवेशिक विरासत से उपजा है जहाँ राज्य की शक्ति को व्यक्तिगत अधिकारों पर प्राथमिकता दी जाती थी। स्वतंत्रता के बाद के युग में भी, राज्य सुरक्षा के औचित्य के तहत नागरिकों की निगरानी की शक्तियों को बनाए रखा गया, जैसा कि भारतीय टेलीग्राफ अधिनियम, 1885 जैसे कानूनों में परिलक्षित होता है।

भारतीय संविधान, हालांकि निजता के अधिकार को स्पष्ट रूप से सूचीबद्ध नहीं करता था, अनुच्छेद 21 ("जीवन और व्यक्तिगत स्वतंत्रता का अधिकार") के तहत इसके निहित अर्थ को धीरे-धीरे न्यायिक व्याख्याओं के माध्यम से विकसित किया गया। प्रारंभिक न्यायिक दृष्टिकोण ने कभी-कभी निजता के अधिकार को कम महत्व दिया (जैसे एम.पी. शर्मा बनाम सतीश चंद्र, 1954 और खड़क सिंह बनाम उत्तर प्रदेश राज्य, 1962), लेकिन बाद के निर्णयों ने इस अधिकार के महत्व को पहचानना शुरू किया। यह पृष्ठभूमि उस संवैधानिक यात्रा को दर्शाती है जिसने अंततः निजता को एक मौलिक अधिकार के रूप में स्थापित करने का मार्ग प्रशस्त किया, जबकि राष्ट्रीय सुरक्षा हमेशा राज्य के एक महत्वपूर्ण और वैध सरोकार के रूप में बनी रही। यह पृष्ठभूमि वर्तमान शोध के लिए वैचारिक आधार प्रदान करती है कि कैसे एक संप्रभु राज्य अपने नागरिकों की सुरक्षा सुनिश्चित करते हुए उनकी व्यक्तिगत स्वतंत्रता का सम्मान करता है।

1.2. पुट्टुस्वामी निर्णय (2017) और भारत में निजता के मौलिक अधिकार की स्थापना:- अगस्त 2017 में, भारत के सर्वोच्च न्यायालय की नौ-न्यायाधीशों की संविधान पीठ ने जस्टिस के.एस. पुट्टुस्वामी (सेवानिवृत्त) और अन्य बनाम भारत संघ और अन्य के ऐतिहासिक मामले में सर्वसम्मति से फैसला सुनाया कि निजता का अधिकार भारतीय संविधान के तहत एक मौलिक अधिकार है। यह निर्णय न केवल भारत में मानवाधिकार न्यायशास्त्र में एक मील का पत्थर था, बल्कि इसने पिछले उन फैसलों को भी प्रभावी रूप से पलट दिया था जो निजता को मौलिक अधिकार नहीं मानते थे।

पुट्टुस्वामी निर्णय ने यह स्पष्ट किया कि निजता अनुच्छेद 21 के तहत जीवन और व्यक्तिगत स्वतंत्रता के अधिकार का एक आंतरिक और अविभाज्य हिस्सा है, और यह संविधान के भाग III के तहत अन्य मौलिक अधिकारों (जैसे अभिव्यक्ति की स्वतंत्रता, संघ बनाने की स्वतंत्रता) के साथ भी जुड़ा हुआ है। इस निर्णय ने निजता के अधिकार पर राज्य द्वारा किसी भी अतिक्रमण के लिए नौ सिद्धांतों का एक सख्त परीक्षण निर्धारित किया: 1. कानूनी वैधता (Legality): कानून का अस्तित्व होना चाहिए। 2. वैध उद्देश्य (Legitimate Aim): राज्य का एक वैध उद्देश्य होना चाहिए। 3. युक्तियुक्तता (Rational Nexus): उद्देश्य और अपनाए गए साधनों के बीच एक युक्तियुक्त संबंध होना चाहिए। 4. आवश्यकता (Necessity): प्राप्त किए जाने वाले उद्देश्य के लिए उपाय आवश्यक होना चाहिए। 5. आनुपातिकता (Proportionality): उपाय की प्रकृति और सीमा उद्देश्य के आनुपातिक होनी चाहिए। 6. न्यूनतम हस्तक्षेप (Least Intrusive): कम से कम हस्तक्षेपकारी साधन अपनाए जाने चाहिए। 7. प्रक्रियात्मक सुरक्षा उपाय (Procedural Safeguards): उचित प्रक्रियागत सुरक्षा उपाय होने चाहिए। 8. गैर-मनमानापन (Non-Arbitrariness): उपाय मनमाना नहीं होना चाहिए। 9. मौलिक अधिकारों का सम्मान (Respect for Fundamental Rights): मौलिक अधिकारों के मूल में निहित मानवीय गरिमा का सम्मान होना चाहिए।

यह निर्णय वर्तमान शोध के लिए आधारशिला है, क्योंकि यह सरकारी निगरानी की वैधता और स्वीकार्यता का मूल्यांकन करने के लिए एक संवैधानिक मापदंड प्रदान करता है।

1.3. डिजिटल युग में निगरानी प्रौद्योगिकियों का उदय और निजता के लिए नई चुनौतियाँ

पुट्टुस्वामी निर्णय ने एक ऐसे समय में निजता को मौलिक अधिकार घोषित किया जब डिजिटल प्रौद्योगिकियाँ अभूतपूर्व गति से विकसित हो रही थीं। इंटरनेट, स्मार्टफोन, सोशल मीडिया प्लेटफॉर्म, इंटरनेट ऑफ थिंग्स (IoT) और कृत्रिम बुद्धिमत्ता (AI) तथा मशीन लर्निंग (ML) जैसी प्रौद्योगिकियों ने मानव संपर्क, डेटा निर्माण और सूचना के प्रसार के तरीके को पूरी तरह से बदल दिया है। इन प्रौद्योगिकियों ने न केवल नागरिकों के लिए अवसर पैदा किए हैं, बल्कि सरकारों के लिए निगरानी की क्षमता को भी नाटकीय रूप से बढ़ा दिया है।

आज, सरकारी एजेंसियाँ बड़े पैमाने पर डेटा (Big Data) का विश्लेषण, फेशियल रिकॉग्निशन तकनीक, स्थान-आधारित ट्रैकिंग, सोशल मीडिया विश्लेषण, और यहां तक कि स्पाइवेयर (जैसे पेगासस) का उपयोग करके नागरिकों की गतिविधियों, संचार और व्यवहार पैटर्न की निगरानी करने में सक्षम हैं। इन उन्नत तकनीकों की विशेषताएं - जैसे उनकी व्यापकता, अदृश्यता, निरंतरता और डेटा के विशाल एकत्रीकरण की क्षमता - निजता के लिए अद्वितीय और गंभीर चुनौतियाँ पैदा करती हैं। ये प्रौद्योगिकियाँ मास सर्विलांस (Mass Surveillance) की संभावना को बढ़ाती हैं, जिससे व्यक्तियों की पहचान के बिना भी उनके जीवन के हर पहलू पर लगातार नज़र रखी जा सकती है। यह 'डिजिटल पैनोप्टिकॉन' का निर्माण करता है, जहाँ नागरिक लगातार निगरानी में होने की भावना के कारण अपनी अभिव्यक्ति की स्वतंत्रता और अन्य मौलिक अधिकारों का प्रयोग करने से कतरा सकते हैं (चिलिंग इफेक्ट)। इस प्रकार, डिजिटल युग ने निजता की पारंपरिक अवधारणाओं और सुरक्षा की आवश्यकताओं को फिर से परिभाषित किया है, जिससे राज्य और नागरिक के बीच संबंधों में एक नया तनाव उत्पन्न हो गया है।

1.4. शोध समस्या और इसके निहितार्थ: वर्तमान कानूनी और संस्थागत ढाँचे की अपर्याप्तता

पुट्टुस्वामी निर्णय और डिजिटल युग में निगरानी प्रौद्योगिकियों के तीव्र विकास के बावजूद, भारत का मौजूदा कानूनी और संस्थागत ढाँचा सरकारी निगरानी को विनियमित करने के लिए गंभीर रूप से अपर्याप्त और पुराना है। वर्तमान में, निगरानी मुख्यतः भारतीय टेलीग्राफ अधिनियम, 1885 की धारा 5 (वायरटैपिंग के लिए) और सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 69 (इलेक्ट्रॉनिक डेटा के अवरोधन, निगरानी और डिक्रिप्शन के लिए) द्वारा शासित होती है। ये कानून डिजिटल युग की जटिलताओं को संबोधित करने के लिए डिज़ाइन नहीं किए गए थे, और वे पुट्टुस्वामी निर्णय द्वारा निर्धारित निजता के सिद्धांतों के साथ अक्सर असंगत पाए जाते हैं।

इन कानूनों में निम्नलिखित प्रमुख कमियाँ हैं: **न्यायिक निरीक्षण का अभाव:** निगरानी आदेश जारी करने का अधिकार कार्यपालिका (गृह मंत्रालय के सचिव स्तर के अधिकारी) के पास रहता है, जिसमें स्वतंत्र न्यायिक प्राधिकरण से पूर्व-अनुमोदन की कमी होती है। **पारदर्शिता की कमी:** निगरानी आदेशों को आमतौर पर गोपनीय रखा जाता है, जिससे सार्वजनिक जवाबदेही और दुरुपयोग की संभावना बढ़ जाती है। **व्यापक विवेक:** कानूनों में

'राष्ट्रीय सुरक्षा' या 'सार्वजनिक व्यवस्था' जैसे शब्दों की अस्पष्ट परिभाषाएँ अधिकारियों को व्यापक और मनमाना विवेक प्रदान करती हैं। **स्वतंत्र निरीक्षण का अभाव:** कोई प्रभावी और स्वतंत्र संस्थागत तंत्र नहीं है जो निगरानी आदेशों की वैधता और आनुपातिकता की समीक्षा कर सके या दुरुपयोग के मामलों की जाँच कर सके। **शिकायत निवारण की कमी:** जिन व्यक्तियों पर निगरानी रखी जाती है, उनके पास आमतौर पर इसके बारे में जानकारी नहीं होती है, जिससे उनके लिए प्रभावी शिकायत निवारण या कानूनी चुनौती देना असंभव हो जाता है। **डेटा संरक्षण सिद्धांतों का एकीकरण नहीं:** नए डिजिटल पर्सनल डेटा प्रोटेक्शन एक्ट, 2023 के बावजूद, सरकारी निगरानी से संबंधित डेटा के संग्रह, उपयोग, प्रतिधारण और विनाश के लिए स्पष्ट और कठोर नियम अनुपस्थित हैं। इन अपर्याप्तताओं के निहितार्थ गंभीर हैं: यह नागरिक स्वतंत्रता के क्षरण, राज्य की शक्ति के संभावित दुरुपयोग, अभिव्यक्ति की स्वतंत्रता पर 'चिलिंग इफेक्ट' और अंतर्राष्ट्रीय मानवाधिकार मानकों के साथ भारत की असंगति की ओर ले जाता है। यह शोध इस गंभीर समस्या पर प्रकाश डालता है और एक संवैधानिक रूप से सुदृढ़, जवाबदेह और प्रभावी नियामक ढाँचे की तत्काल आवश्यकता को रेखांकित करता है।

1.5. शोध प्रश्न (Research Questions): इस शोध पत्र का उद्देश्य निम्नलिखित केंद्रीय प्रश्नों का उत्तर देना है:

डिजिटल युग में भारत में सरकारी निगरानी की प्रकृति और सीमाएँ क्या हैं?

- यह प्रश्न भारत में सरकार द्वारा उपयोग की जा रही विभिन्न निगरानी प्रौद्योगिकियों (जैसे AI, फेशियल रिकॉग्निशन, बिग डेटा विश्लेषण) और उनके संचालन के तरीकों का मानचित्रण करना चाहता है, साथ ही यह भी विश्लेषण करता है कि ये प्रौद्योगिकियाँ पारंपरिक निगरानी से किस प्रकार भिन्न हैं और निजता के लिए क्या नई चुनौतियाँ प्रस्तुत करती हैं।

मौजूदा भारतीय कानूनी और संस्थागत ढाँचा पुट्टुस्वामी निर्णय द्वारा स्थापित निजता के सिद्धांतों के साथ कहाँ तक संरेखित होता है?

- यह प्रश्न वर्तमान कानूनों (भारतीय टेलीग्राफ अधिनियम, आईटी अधिनियम की धारा 69) और उनसे संबंधित नियमों तथा प्रशासनिक प्रक्रियाओं का एक गंभीर मूल्यांकन करेगा, यह निर्धारित करने के लिए कि वे पुट्टुस्वामी निर्णय में निर्धारित आनुपातिकता, आवश्यकता, वैध उद्देश्य और प्रक्रियात्मक सुरक्षा उपायों जैसे सिद्धांतों को कितना पूरा करते हैं।

कौन से अंतरराष्ट्रीय सर्वोत्तम अभ्यास भारत के लिए एक प्रभावी और संवैधानिक रूप से सुदृढ़ नियामक ढाँचा बनाने में उपयोगी हो सकते हैं?

- यह प्रश्न अन्य लोकतांत्रिक न्यायक्षेत्रों (जैसे यूरोपीय संघ, संयुक्त राज्य अमेरिका, यूनाइटेड किंगडम) में अपनाए गए सरकारी निगरानी कानूनों और निरीक्षण तंत्रों का एक तुलनात्मक विश्लेषण करेगा, ताकि भारत के लिए प्रासंगिक और अनुकूलनीय मॉडल, सिद्धांत और सुरक्षा उपायों की पहचान की जा सके।

भारत में निजता के अधिकार का सम्मान करते हुए राष्ट्रीय सुरक्षा हितों को संबोधित करने वाला एक नवीन नियामक ढाँचा कैसा दिख सकता है?

- इन विश्लेषणात्मक निष्कर्षों के आधार पर, यह प्रश्न एक व्यापक, संवैधानिक रूप से वैध और तकनीकी रूप से जागरूक नियामक ढाँचे का प्रस्ताव करेगा, जिसमें कठोर न्यायिक या स्वतंत्र निरीक्षण, पारदर्शिता, जवाबदेही और प्रभावी शिकायत निवारण तंत्र शामिल होंगे, जो डिजिटल युग में निजता और राष्ट्रीय सुरक्षा के बीच संतुलन स्थापित कर सकें।

1.6. शोध का दायरा और सीमाएँ

- दायरा (Scope): यह शोध मुख्य रूप से भारत में सरकारी निगरानी पर केंद्रित है, जिसमें राज्य एजेंसियों द्वारा राष्ट्रीय सुरक्षा के नाम पर व्यक्तिगत डेटा और संचार के संग्रह, प्रसंस्करण और उपयोग के कानूनी, संवैधानिक और नीतिगत पहलू शामिल हैं। इसमें डिजिटल निगरानी प्रौद्योगिकियों का विशेष रूप से विश्लेषण किया जाएगा। तुलनात्मक विश्लेषण के लिए, प्रमुख लोकतांत्रिक देशों के निगरानी कानूनों और प्रथाओं का अध्ययन किया जाएगा।

सीमाएँ (Limitations):

- यह शोध मुख्य रूप से सैद्धांतिक-कानूनी और नीतिगत विश्लेषण पर आधारित होगा। निगरानी गतिविधियों पर गोपनीय या वर्गीकृत जानकारी तक पहुँच की कमी के कारण, वास्तविक समय के संचालन या मात्रात्मक डेटा का विश्लेषण सीमित हो सकता है।
- साइबर सुरक्षा के तकनीकी पहलुओं का विश्लेषण कानून और नीति के संदर्भ में किया जाएगा, न कि गहन तकनीकी विशेषज्ञता के दृष्टिकोण से।
- यह शोध मुख्य रूप से भारत के भीतर सरकारी निगरानी पर केंद्रित है और निजी क्षेत्र की निगरानी प्रथाओं को केवल तभी कवर करेगा जब वे सरकारी एजेंसियों के साथ डेटा साझा करने या उनके निर्देशों के तहत काम

करने से संबंधित हों।
- राष्ट्रीय सुरक्षा के विषय की संवेदनशीलता और इसमें शामिल भू-राजनीतिक कारकों को स्वीकार करते हुए, शोध का ध्यान संवैधानिक और कानूनी संतुलन बनाए रखने पर रहेगा।

1.7. कार्यप्रणाली (Methodology)

यह शोध एक बहु-आयामी दृष्टिकोण अपनाएगा जिसमें निम्नलिखित शामिल हैं:
- **सैद्धांतिक-कानूनी विश्लेषण (Doctrinal Legal Analysis):** इसमें भारतीय संविधान के प्रावधानों, सर्वोच्च न्यायालय के निर्णयों (विशेषकर पुट्टुस्वामी निर्णय), विभिन्न कानूनों (जैसे भारतीय टेलीग्राफ अधिनियम, आईटी अधिनियम, डीपीआर एक्ट) और संबंधित नियमों का गहन अध्ययन शामिल होगा। इसका उद्देश्य भारत में निजता और निगरानी से संबंधित कानूनी ढाँचे को समझना और उसकी व्याख्या करना है।
- **तुलनात्मक विश्लेषण (Comparative Analysis):** यह कार्यप्रणाली विभिन्न लोकतांत्रिक न्यायक्षेत्रों (जैसे यूरोपीय संघ, संयुक्त राज्य अमेरिका, यूनाइटेड किंगडम) में सरकारी निगरानी के कानूनी और संस्थागत ढाँचे की जाँच करेगी। इसका लक्ष्य सर्वोत्तम अभ्यासों, नियामक मॉडलों और स्वतंत्र निरीक्षण तंत्रों की पहचान करना है जो भारत के लिए प्रासंगिक हो सकते हैं।
- **नीति विश्लेषण (Policy Analysis):** यह भारत सरकार द्वारा जारी विभिन्न रिपोर्टों, श्वेत पत्रों, प्रस्तावित बिलों और नीतिगत दस्तावेजों का विश्लेषण करेगा, जो निगरानी और डेटा संरक्षण से संबंधित हैं। इसका उद्देश्य मौजूदा नीतिगत दिशाओं और उनकी प्रभावकारिता का मूल्यांकन करना है।
- **अंतःविषयक दृष्टिकोण (Interdisciplinary Approach):** शोध को केवल कानूनी दृष्टिकोण तक सीमित न रखकर, यह लोक नीति (शासन, जवाबदेही), राजनीतिक विज्ञान (राज्य शक्ति, लोकतंत्र), साइबर सुरक्षा (तकनीकी क्षमताएं, कमजोरियां) और नैतिकता (मानवाधिकार, न्याय) के क्षेत्रों से अंतर्दृष्टि प्राप्त करेगा। यह दृष्टिकोण शोध समस्या की जटिलता को व्यापक रूप से समझने में मदद करेगा।

1.8. शोध का महत्व (Significance)

यह शोध कई स्तरों पर महत्वपूर्ण योगदान देगा:
- **शैक्षणिक योगदान (Academic Contribution):** यह पुट्टुस्वामी निर्णय के बाद भारत में निजता और राष्ट्रीय सुरक्षा पर मौजूदा साहित्य में एक महत्वपूर्ण अंतर को भरेगा। यह सरकारी निगरानी के कानूनी, संवैधानिक, तकनीकी और नैतिक आयामों का एक व्यापक और अद्यतन विश्लेषण प्रस्तुत करेगा, जिससे इस क्षेत्र में भविष्य के शोध के लिए एक आधार तैयार होगा। यह प्रस्तावित नवीन नियामक ढाँचा अकादमिक विमर्श को समृद्ध करेगा।
- **नीतिगत सिफारिशें (Policy Recommendations):** शोध के निष्कर्ष भारत में नीति निर्माताओं को डिजिटल युग में सरकारी निगरानी को विनियमित करने के लिए अधिक प्रभावी, पारदर्शी और संवैधानिक रूप से अनुरूप कानूनी और संस्थागत ढाँचा विकसित करने में मार्गदर्शन प्रदान करेंगे। यह नीतिगत संवाद को मजबूत करने और संभावित कानूनी सुधारों को सूचित करने में मदद करेगा।
- **सार्वजनिक विमर्श को बढ़ावा देना (Fostering Public Discourse):** यह शोध नागरिकों, नागरिक समाज संगठनों और मीडिया के बीच निजता के अधिकार, राष्ट्रीय सुरक्षा की आवश्यकताओं और सरकारी निगरानी के निहितार्थों के बारे में जागरूकता बढ़ाएगा। एक सूचित सार्वजनिक विमर्श लोकतांत्रिक जवाबदेही के लिए महत्वपूर्ण है और यह सुनिश्चित करने में मदद करता है कि राज्य की शक्ति का उपयोग जिम्मेदारी से किया जाए।
- **लोकतांत्रिक मूल्यों की सुरक्षा (Safeguarding Democratic Values):** अंततः, यह शोध एक ऐसे संतुलन की तलाश करता है जो एक जीवंत लोकतंत्र के लिए आवश्यक व्यक्तिगत स्वतंत्रता और सुरक्षा के बीच सामंजस्य स्थापित करे। यह सुनिश्चित करने में योगदान देगा कि भारत एक डिजिटल दुनिया में अपने संवैधानिक मूल्यों और नागरिक स्वतंत्रता को बरकरार रखे।

2: निजता, राष्ट्रीय सुरक्षा और निगरानी के वैचारिक आधार (Conceptual Foundations of Privacy, National Security, and Surveillance): यह शोध पत्र के तीन केंद्रीय स्तंभों – निजता (Privacy), राष्ट्रीय सुरक्षा (National Security) और निगरानी (Surveillance) – की सैद्धांतिक नींव की पड़ताल करता है। यह इन अवधारणाओं की बहुआयामी प्रकृति को स्पष्ट करेगा, विभिन्न दार्शनिक और कानूनी दृष्टिकोणों को प्रस्तुत करेगा, और इनके बीच के अंतर्निहित तनाव को उजागर करेगा, जो एक संवैधानिक लोकतंत्र के लिए केंद्रीय है।

2.1. निजता की अवधारणा: विभिन्न दार्शनिक और कानूनी दृष्टिकोण (प्रोसर, वेस्टिन, सोलोव)

निजता एक जटिल और बहुआयामी अवधारणा है जिसका कोई सार्वभौमिक रूप से स्वीकृत एकल परिभाषा नहीं

है। यह ऐतिहासिक रूप से, सांस्कृतिक रूप से और तकनीकी विकास के साथ बदलती रही है। दार्शनिक रूप से, निजता को स्वायत्तता (autonomy), गरिमा (dignity) और व्यक्ति के स्वयं पर नियंत्रण के अधिकार से जोड़ा गया है। कानूनी रूप से, इसे अक्सर अन्य अधिकारों, जैसे स्वतंत्रता, अभिव्यक्ति और साहचर्य, के अग्रदूत के रूप में देखा जाता है।

प्रोसर का दृष्टिकोण (Prosser's View): विलियम एल. प्रोसर (William L. Prosser) ने 1960 में निजता के अपकृत्य (tort of privacy) को चार अलग-अलग श्रेणियों में विभाजित किया था, जिससे निजता को कानूनी रूप से पहचानने में मदद मिली:

1. **सार्वजनिक प्रकटीकरण (Public Disclosure):** किसी के निजी मामलों का सार्वजनिक रूप से अपमानजनक तरीके से प्रकाशन।
2. **झूठा प्रकाश (False Light):** किसी के बारे में गलत जानकारी का प्रकाशन जो उन्हें झूठी रोशनी में प्रस्तुत करता है (हालांकि यह मानहानि से अलग है)।
3. **अतिक्रमण (Intrusion upon Seclusion):** किसी व्यक्ति के एकांत या निजी मामलों में शारीरिक या इलेक्ट्रॉनिक रूप से घुसपैठ करना।
4. **नाम या समानता का विनियोग (Appropriation of Name or Likeness):** किसी के नाम या समानता का वाणिज्यिक लाभ के लिए उपयोग करना। प्रोसर का काम निजता को एक सुरक्षात्मक अधिकार के रूप में स्थापित करता है जो व्यक्तियों को दूसरों के अनुचित हस्तक्षेप से बचाता है।

- **वेस्टिन का दृष्टिकोण (Westin's View):** एलन वेस्टिन (Alan Westin) ने 1967 में अपनी प्रभावशाली पुस्तक "प्राइवेसी एंड फ्रीडम" में निजता को "सूचना पर व्यक्तियों, समूहों या संस्थाओं के दावे के रूप में परिभाषित किया, ताकि यह तय किया जा सके कि अपने बारे में कितनी जानकारी दूसरों को दी जाए, कब और कैसे।" उन्होंने निजता को चार कार्यात्मक राज्यों में देखा: एकांत (solitude), अंतरंगता (intimacy), गुमनामी (anonymity) और आरक्षितता (reserve)। वेस्टिन का जोर व्यक्ति के सूचनात्मक स्वयं (informational self) पर नियंत्रण पर था, जो सूचनात्मक निजता (informational privacy) की आधुनिक अवधारणा का आधार बना।
- **सोलोव का दृष्टिकोण (Solove's View):** डैनियल जे. सोलोव (Daniel J. Solove) ने 21वीं सदी में निजता पर व्यापक काम किया है, यह तर्क देते हुए कि निजता एक एकल, एकीकृत अवधारणा नहीं है, बल्कि संबंधित समस्याओं का एक समूह है। उन्होंने निजता उल्लंघनों के लिए एक व्यापक वर्गीकरण प्रस्तावित किया है, जिसमें सूचना एकत्र करना (जैसे निगरानी, पूछताछ), सूचना प्रसंस्करण (जैसे एकत्रीकरण, पहचान, भेदभाव), सूचना प्रसार (जैसे प्रकटीकरण, अपमान, ब्लैकलिस्टिंग), और आक्रमण (जैसे घुसपैठ, ज़बरदस्ती) शामिल हैं। सोलोव का दृष्टिकोण निजता के खतरों की बहुलता को पहचानता है और यह दर्शाता है कि कैसे डिजिटल युग में ये खतरे कई रूपों में प्रकट होते हैं।
- **भारत के संदर्भ में निजता की बहुआयामी प्रकृति:** पुट्टुस्वामी निर्णय ने भारत में निजता की बहुआयामी प्रकृति को स्पष्ट रूप से स्वीकार किया। यह केवल एकांत में रहने का अधिकार नहीं है, बल्कि इसमें कई पहलू शामिल हैं:

a) **भौतिक निजता (Physical Privacy):** व्यक्ति के शरीर और निजी स्थान (जैसे घर) में अनाधिकृत प्रवेश से स्वतंत्रता। इसमें शारीरिक अखंडता और व्यक्तिगत स्वायत्तता शामिल है।

b) **सूचनात्मक निजता (Informational Privacy):** व्यक्तियों की अपनी व्यक्तिगत जानकारी पर नियंत्रण रखने की क्षमता, जिसमें उनका डेटा कैसे एकत्र किया जाता है, उपयोग किया जाता है, संग्रहीत किया जाता है और साझा किया जाता है, यह तय करने का अधिकार शामिल है। डिजिटल युग में यह सबसे महत्वपूर्ण पहलू है।

c) **पहचान संबंधी निजता (Identity Privacy):** किसी की व्यक्तिगत पहचान पर नियंत्रण, जिसमें यौन अभिविन्यास, राजनीतिक विश्वास, धार्मिक संबद्धता और अन्य व्यक्तिगत विशेषताएँ शामिल हैं। यह व्यक्ति के स्वयं-निर्धारण (self-determination) के अधिकार से निकटता से जुड़ा है।

d) **निर्णय संबंधी निजता (Decisional Privacy):** जीवन के महत्वपूर्ण व्यक्तिगत निर्णयों (जैसे विवाह, प्रजनन अधिकार, जीवन शैली) में राज्य के हस्तक्षेप से स्वतंत्रता।

e) **संचार निजता (Communicational Privacy):** संचार की गोपनीयता और यह सुनिश्चित करने का अधिकार कि निजी बातचीत को बिना सहमति के अवरोधित या प्रकट न किया जाए। यह बहुआयामी समझ भारत में निजता के अधिकार पर राज्य द्वारा किसी भी हस्तक्षेप की वैधता का मूल्यांकन करने के लिए एक मजबूत

आधार प्रदान करती है।

2.2. राष्ट्रीय सुरक्षा की अवधारणा: परिभाषाएँ, सीमाएँ और राज्य की वैध चिंताएँ

राष्ट्रीय सुरक्षा एक जटिल और अक्सर विवादास्पद अवधारणा है, जो राज्य के अस्तित्व और कल्याण से जुड़ी है। परंपरागत रूप से, इसे बाहरी खतरों (जैसे युद्ध, आतंकवाद, जासूसी) से राज्य की रक्षा करने और आंतरिक स्थिरता बनाए रखने की क्षमता के रूप में परिभाषित किया गया है। इसमें संप्रभुता (sovereignty), क्षेत्रीय अखंडता (territorial integrity), राजनीतिक स्थिरता और नागरिकों की सुरक्षा शामिल है।

परिभाषाएँ और राज्य की वैध चिंताएँ:

- रक्षात्मक आयाम: सशस्त्र आक्रमण, बाहरी हस्तक्षेप और भू-राजनीतिक प्रतिद्वंद्विता से राज्य की सीमाओं और संस्थानों की रक्षा करना।
- आंतरिक सुरक्षा आयाम: आतंकवाद, उग्रवाद, सांप्रदायिक हिंसा, संगठित अपराध और साइबर हमलों जैसे आंतरिक खतरों से कानून और व्यवस्था बनाए रखना।
- आर्थिक सुरक्षा: महत्वपूर्ण आर्थिक बुनियादी ढाँचे और वित्तीय प्रणालियों को सुरक्षित रखना।
- ऊर्जा और खाद्य सुरक्षा: देश के लिए महत्वपूर्ण संसाधनों की उपलब्धता सुनिश्चित करना।
- साइबर सुरक्षा: महत्वपूर्ण सूचना अवसंरचना और डिजिटल प्रणालियों को साइबर हमलों से बचाना। ये सभी राज्य की वैध चिंताएँ हैं, जिनके लिए राज्य को कुछ विशेष शक्तियों और संसाधनों से लैस होना आवश्यक है, जिसमें कभी-कभी निगरानी की क्षमता भी शामिल होती है।

अस्पष्ट परिभाषाओं का दुरुपयोग और 'सुरक्षा' के नाम पर अधिकारों का हनन: राष्ट्रीय सुरक्षा की अवधारणा की समस्या इसकी अंतर्निहित अस्पष्टता में निहित है। 'राष्ट्रीय सुरक्षा' या 'सार्वजनिक व्यवस्था' जैसे शब्द अक्सर व्यापक और अस्पष्ट होते हैं, जिससे कार्यपालिका को मनमाने ढंग से शक्ति का प्रयोग करने का बहाना मिल जाता है। इस अस्पष्टता के कई गंभीर परिणाम हो सकते हैं:

- अधिकारों का हनन: 'सुरक्षा' के नाम पर, राज्य नागरिकों के मौलिक अधिकारों, विशेषकर निजता, अभिव्यक्ति की स्वतंत्रता और विरोध के अधिकार पर अतिक्रमण कर सकता है। असहमति, आलोचना या वैध विरोध को अक्सर राष्ट्रीय सुरक्षा के लिए खतरे के रूप में पेश किया जा सकता है।
- जवाबदेही की कमी: राष्ट्रीय सुरक्षा के मामलों को अक्सर गोपनीयता के आवरण में रखा जाता है, जिससे न्यायिक और संसदीय निरीक्षण मुश्किल हो जाता है। इससे सरकारी अधिकारियों को बिना पर्याप्त जाँच के कार्य करने की छूट मिल जाती है।
- शक्ति का दुरुपयोग: अस्पष्ट शक्तियाँ सत्तावादी प्रवृत्तियों को बढ़ावा दे सकती हैं और नागरिक समाज को कमजोर कर सकती हैं। इतिहास गवाह है कि कई बार सरकारों ने अपने राजनीतिक विरोधियों या असंतोष को दबाने के लिए सुरक्षा कानूनों का दुरुपयोग किया है।
- डर का माहौल: जब नागरिक यह महसूस करते हैं कि उन पर लगातार निगरानी रखी जा रही है, तो यह 'चिलिंग इफेक्ट' पैदा कर सकता है, जिससे वे अपने वैध अधिकारों का प्रयोग करने से भी डरते हैं।

इसलिए, एक संवैधानिक लोकतंत्र में, राष्ट्रीय सुरक्षा की अवधारणा को स्पष्ट रूप से परिभाषित करना, उसकी सीमाओं को निर्धारित करना और उसके अभ्यास के लिए कठोर सुरक्षा उपाय प्रदान करना अत्यंत महत्वपूर्ण है ताकि अधिकारों का हनन न हो।

2.3. निगरानी की प्रकृति और उसके प्रकार: पारंपरिक से डिजिटल निगरानी तक का विकास

निगरानी से तात्पर्य व्यक्तियों, समूहों या स्थानों पर जानकारी एकत्र करने, संसाधित करने और विश्लेषण करने के व्यवस्थित अवलोकन से है। यह व्यक्तियों के व्यवहार को प्रभावित करने, खतरे की पहचान करने या कानून लागू करने के उद्देश्य से किया जाता है। निगरानी ने पारंपरिक तरीकों से लेकर डिजिटल युग की अत्याधुनिक तकनीकों तक एक लंबा सफर तय किया है।

पारंपरिक निगरानी (Traditional Surveillance):

- शारीरिक अवलोकन: जासूस, गुप्तचरों द्वारा व्यक्तियों का पीछा करना, बैठकों का अवलोकन करना।
- वायरटैपिंग (Wiretapping): टेलीफोन लाइनों को टैप करके बातचीत सुनना (जैसे भारतीय टेलीग्राफ अधिनियम के तहत)।
- मेल इंटरसेप्शन: डाक द्वारा भेजे गए पत्रों को खोलना और पढ़ना।
- गुपचुप खोज (Covert Searches): घरों या कार्यालयों में घुसकर जानकारी एकत्र करना। ये तरीके अक्सर श्रम-गहन, सीमित दायरे वाले और विशिष्ट व्यक्तियों पर लक्षित होते थे।

डिजिटल निगरानी (Digital Surveillance): डिजिटल युग ने निगरानी की प्रकृति को मौलिक रूप से बदल दिया

है। यह अब केवल शारीरिक अवलोकन तक सीमित नहीं है, बल्कि यह अदृश्य, व्यापक, स्वचालित और अत्यधिक डेटा-गहन हो गया है।

- इंटरनेट इंटरसेप्शन: ईमेल, चैट, वेब ब्राउजिंग इतिहास और ऑनलाइन गतिविधियों की निगरानी।
- मोबाइल फोन ट्रैकिंग: कॉल रिकॉर्ड, संदेश, स्थान डेटा और ऐप उपयोग की निगरानी।
- डिजिटल फोरेंसिक: इलेक्ट्रॉनिक उपकरणों से डेटा निकालना और उसका विश्लेषण करना।
- डेटा माइनिंग और एनालिटिक्स: बड़ी मात्रा में डिजिटल डेटा का विश्लेषण करके पैटर्न और संबंध खोजना।

निगरानी के प्रमुख प्रकार डिजिटल युग में:

1. मास सर्विलांस (Mass Surveillance): यह एक ऐसी प्रणाली है जहाँ राज्य एजेंसियाँ या अन्य संस्थाएँ, पूर्व संदेह के बिना, बड़ी आबादी से व्यापक पैमाने पर डेटा एकत्र करती हैं, जिसे अक्सर ' blanket surveillance' भी कहा जाता है। इसका उद्देश्य संभावित खतरों का पता लगाने के लिए बड़े डेटासेट में पैटर्न की पहचान करना है।

- विशेषताएँ: गैर-लक्षित, स्वचालित, विशाल डेटा एकत्रीकरण, अक्सर अदृश्य।
- उदाहरण: सभी इंटरनेट ट्रैफ़िक का संग्रह, सार्वजनिक स्थानों पर व्यापक सीसीटीवी नेटवर्क के माध्यम से फेशियल रिकॉग्निशन, दूरसंचार कंपनियों से थोक मेटाडेटा का संग्रह।
- निजता पर प्रभाव: यह 'चिलिंग इफेक्ट' पैदा करता है, व्यक्तिगत स्वायत्तता का हनन करता है, और संभावित रूप से भेदभावपूर्ण प्रोफाइलिंग को जन्म देता है।

2. टार्गेटेड सर्विलांस (Targeted Surveillance): यह विशिष्ट व्यक्तियों या समूहों पर आधारित होती है, जिनके बारे में यह मानने का उचित आधार होता है कि वे किसी अपराध या राष्ट्रीय सुरक्षा के लिए खतरे में शामिल हैं। इसमें न्यायिक या कार्यकारी प्राधिकरण द्वारा जारी एक विशिष्ट वारंट की आवश्यकता होती है।

- विशेषताएँ: विशिष्ट व्यक्ति पर लक्षित, वारंट-आधारित, अधिक सीमित दायरे वाला।
- उदाहरण: किसी संदिग्ध आतंकवादी के फोन पर टैप करना, किसी विशिष्ट वेबसाइट की गतिविधियों की निगरानी करना।
- निजता पर प्रभाव: यह निजता पर कम व्यापक हमला है, लेकिन यदि उचित सुरक्षा उपाय नहीं हों तो इसका भी दुरुपयोग हो सकता है।

3.मेटाडेटा (Metadata) का विश्लेषण: मेटाडेटा "डेटा के बारे में डेटा" है। यह संचार की सामग्री नहीं, बल्कि उसके आसपास की जानकारी है (जैसे किसने किसे कब, कहाँ और कितनी देर बात की; कौन सी वेबसाइट कब देखी गई)।

- विशेषताएँ: कम 'घुसपैठिया' प्रतीत होता है, लेकिन अत्यधिक खुलासा करने वाला। मेटाडेटा का विश्लेषण करके किसी व्यक्ति के व्यवहार, संबंधों, राजनीतिक झुकावों और निजी जीवन के बारे में आश्चर्यजनक रूप से विस्तृत प्रोफाइल बनाई जा सकती है।
- उदाहरण: फोन कॉल लॉग, ईमेल हेडर, आईपी एड्रेस, स्थान डेटा, वेब ब्राउजिंग रिकॉर्ड।
- निजता पर प्रभाव: हालांकि यह संचार की सामग्री नहीं है, मेटाडेटा का एकत्रीकरण और विश्लेषण व्यक्ति की निजता पर उतना ही या उससे भी अधिक गंभीर अतिक्रमण कर सकता है, क्योंकि यह बड़े पैमाने पर लोगों के नेटवर्क और आदतों को उजागर कर सकता है। पुट्टुस्वामी निर्णय ने भी मेटाडेटा को निजता के दायरे में माना है।

2.4. फूकॉल्ट का पैनोप्टिकॉन और डिजिटल पैनोप्टिकॉन की अवधारणा

फूकॉल्ट का पैनोप्टिकॉन (Foucault's Panopticon): फ्रांसीसी दार्शनिक मिशेल फूकॉल्ट (Michel Foucault) ने अपनी पुस्तक "डिसिप्लिन एंड पनिश: द बर्थ ऑफ द प्रिजन" (1975) में जेरेमी बेंथम (Jeremy Bentham) द्वारा डिज़ाइन की गई एक विशेष जेल वास्तुकला, पैनोप्टिकॉन, की अवधारणा का विश्लेषण किया। पैनोप्टिकॉन एक गोलाकार संरचना है जिसमें एक केंद्रीय निगरानी टॉवर होता है जो सभी कैदी कोठरियों को देखता है। कैदी केंद्रीय टॉवर को नहीं देख सकते, जिससे उन्हें यह पता नहीं चलता कि उन्हें कब देखा जा रहा है।

- **मुख्य विचार:** इस डिज़ाइन का उद्देश्य कैदियों के दिमाग में निरंतर निगरानी की भावना पैदा करना है, चाहे वास्तव में कोई उन्हें देख रहा हो या नहीं। इस निरंतर देखने की संभावना के कारण, कैदी स्वयं को अनुशासित करते हैं और मानदंडों के अनुसार व्यवहार करते हैं। फूकॉल्ट के लिए, पैनोप्टिकॉन शक्ति का एक रूपक था जो संस्थानों (जैसे जेल, स्कूल, अस्पताल, कारखाने) में नियंत्रण और आत्म-अनुशासन को लागू करता है, जहाँ शक्ति अदृश्य होती है लेकिन सर्वव्यापी महसूस होती है।

डिजिटल पैनोप्टिकॉन की अवधारणा (Concept of Digital Panopticon): डिजिटल युग में, प्रौद्योगिकी ने एक पैनोप्टिकॉन के निर्माण को संभव बना दिया है जो बेंथम की कल्पना से कहीं अधिक व्यापक और सूक्ष्म है। 'डिजिटल

पैनोप्टिकॉन' वह स्थिति है जहाँ व्यक्ति अपनी सहमति के बिना या अपनी जानकारी के बिना, लेकिन डेटा एकत्र करने वाले उपकरणों और प्रणालियों के माध्यम से लगातार निगरानी में होते हैं।

- **प्रौद्योगिकी का योगदान:** स्मार्टफोन, इंटरनेट ऑफ थिंग्स (IoT) उपकरण, सीसीटीवी कैमरे, सोशल मीडिया, ऑनलाइन ट्रैकिंग कुकीज़, फेशियल रिकॉग्निशन सिस्टम और बिग डेटा विश्लेषण जैसी प्रौद्योगिकियाँ प्रत्येक ऑनलाइन क्लिक, खरीदारी, स्थान और संचार को रिकॉर्ड कर सकती हैं।

विशेषताएँ:

a) **अदृश्यता और सर्वव्यापकता:** निगरानी अक्सर अदृश्य होती है और हर जगह मौजूद होती है।
b) **निरंतरता:** डेटा 24/7 एकत्र किया जा सकता है।
c) **अनिश्चितता:** व्यक्तियों को पता नहीं होता कि उनका डेटा कब, किसके द्वारा और किस उद्देश्य से एकत्र किया जा रहा है।
d) **आत्म-सेंसरशिप:** निरंतर निगरानी के डर से व्यक्ति अपनी अभिव्यक्ति, अन्वेषण या गैर-अनुरूपता को सीमित कर सकते हैं, जिससे लोकतंत्र के लिए आवश्यक असहमति और विविधता दब जाती है। डिजिटल पैनोप्टिकॉन राज्य और कॉर्पोरेट दोनों द्वारा संचालित हो सकता है, जिससे निजता और व्यक्तिगत स्वतंत्रता के लिए गंभीर खतरा उत्पन्न होता है। यह अवधारणा इस शोध के लिए महत्वपूर्ण है क्योंकि यह आधुनिक निगरानी के मनोवैज्ञानिक और सामाजिक प्रभावों को समझने में मदद करती है।

2.5. संवैधानिक लोकतंत्र में संतुलनकारी कार्य: स्वतंत्रता और सुरक्षा के बीच आदर्श संबंध

एक संवैधानिक लोकतंत्र के लिए स्वतंत्रता (Liberty) और सुरक्षा (Security) के बीच सही संतुलन खोजना एक मौलिक और शाश्वत चुनौती है। दोनों ही लोकतांत्रिक शासन के लिए आवश्यक हैं, लेकिन उनके बीच अक्सर तनाव बना रहता है।

- **स्वतंत्रता का महत्व:** लोकतंत्र व्यक्ति की स्वायत्तता, आत्म-अभिव्यक्ति और गरिमा पर आधारित है। मौलिक अधिकार (जैसे निजता, भाषण, संघ) नागरिकों को राज्य की मनमानी शक्ति से बचाते हैं और उन्हें एक पूर्ण जीवन जीने में सक्षम बनाते हैं। अधिक स्वतंत्रता एक रचनात्मक, विविध और जीवंत समाज को बढ़ावा देती है।
- **सुरक्षा का महत्व:** राज्य का प्राथमिक कार्य अपने नागरिकों को बाहरी और आंतरिक खतरों से बचाना है। सुरक्षा के अभाव में, नागरिकों की स्वतंत्रता का कोई मतलब नहीं रह जाता। एक सुरक्षित वातावरण ही व्यक्तियों को अपने अधिकारों का प्रयोग करने और समाज में भाग लेने में सक्षम बनाता है।
- **संतुलनकारी कार्य:** आदर्श रूप से, स्वतंत्रता और सुरक्षा परस्पर पूरक होने चाहिए, एक दूसरे को मजबूत करना चाहिए। हालांकि, व्यवहार में, राज्य अक्सर सुरक्षा के नाम पर स्वतंत्रता पर अतिक्रमण करने के लिए प्रवृत्त होता है। संवैधानिक लोकतंत्र में, यह संतुलन निम्नलिखित के माध्यम से प्राप्त किया जाता है:

a) **कानून का शासन (Rule of Law):** राज्य की सभी शक्तियाँ कानून द्वारा सीमित होनी चाहिए और मनमानी नहीं होनी चाहिए।
b) **मौलिक अधिकार:** संविधान में अधिकारों को निहित करना और उन्हें राज्य द्वारा अतिक्रमण से बचाना।
c) **शक्ति पृथक्करण (Separation of Powers):** कार्यपालिका, विधायिका और न्यायपालिका के बीच शक्ति का विभाजन ताकि कोई भी शाखा अत्यधिक शक्तिशाली न हो सके।
d) **न्यायिक समीक्षा (Judicial Review):** न्यायपालिका की यह शक्ति कि वह सरकारी कार्यों और कानूनों की संवैधानिकता की जाँच करे।
e) **जवाबदेही और पारदर्शिता:** सरकार के कार्यों को सार्वजनिक निरीक्षण के अधीन रखना और उन्हें जवाबदेह बनाना।
f) **आनुपातिकता का सिद्धांत:** राज्य द्वारा अधिकारों पर लगाए गए किसी भी प्रतिबंध को एक वैध उद्देश्य को प्राप्त करने के लिए आवश्यक और उस उद्देश्य के आनुपातिक होना चाहिए।

3.1. ऐतिहासिक पृष्ठभूमि: औपनिवेशिक विरासत और स्वतंत्रता के बाद के कानून:-

- औपनिवेशिक विरासत: भारत में निगरानी कानूनों की जड़ें ब्रिटिश काल में हैं। ब्रिटिश सरकार ने भारतीय टेलीग्राफ अधिनियम, 1885 जैसे कानून मुख्य रूप से भारतीय राष्ट्रवादियों की गतिविधियों पर नज़र रखने और औपनिवेशिक शासन के विरुद्ध विद्रोह को रोकने के लिए बनाए थे। इन कानूनों में 'सार्वजनिक आपातकाल' (Public Emergency) जैसे अस्पष्ट शब्द शामिल थे, जो राज्य को व्यापक शक्तियाँ देते थे।
- स्वतंत्रता के बाद निरंतरता: स्वतंत्रता के बाद, भारतीय राज्य ने इन औपनिवेशिक कानूनों को बड़े पैमाने पर बरकरार रखा। हालाँकि संविधान ने मौलिक अधिकार प्रदान किए, लेकिन राज्य ने राष्ट्रीय सुरक्षा और अखंडता के नाम पर निगरानी की शक्तियों को बनाए रखना आवश्यक समझा। समय के साथ, तकनीकी प्रगति के साथ

तालमेल बिठाने के लिए नए कानून (जैसे आईटी अधिनियम) जोड़े गए, लेकिन नियंत्रण का मूल दर्शन अक्सर कार्यपालिका-केंद्रित ही रहा।

3.2. प्रमुख कानूनी प्रावधान (Key Legal Provisions):- भारत में निगरानी मुख्य रूप से दो प्रमुख कानूनों और उनके संबंधित नियमों द्वारा संचालित होती है:

- **भारतीय टेलीग्राफ अधिनियम, 1885 (Section 5(2)):**

a) यह धारा सरकार को "सार्वजनिक आपातकाल" या "सार्वजनिक सुरक्षा" के हित में संदेशों को अवरुद्ध (Intercept) करने की अनुमति देती है।

b) नियम 419A: पीयूसीएल मामले (1996) के बाद जोड़े गए ये नियम अवरोधन के लिए प्रक्रिया निर्धारित करते हैं, जिसमें गृह सचिव की अनुमति आवश्यक होती है।

- **सूचना प्रौद्योगिकी अधिनियम, 2000 (Section 69):**

a) यह डिजिटल युग का प्राथमिक कानून है। धारा 69 सरकार को किसी भी कंप्यूटर संसाधन के माध्यम से प्रेषित जानकारी को अवरुद्ध करने, निगरानी करने या डिक्रिप्ट (Decrypt) करने की शक्ति देती है।

b) इसका दायरा टेलीग्राफ अधिनियम से व्यापक है क्योंकि इसमें "अपराध की जाँच" को भी एक आधार के रूप में शामिल किया गया है।

c) IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009: ये नियम निगरानी की प्रक्रियात्मक रूपरेखा तय करते हैं।

- **आपराधिक प्रक्रिया संहिता, 1973 (CrPC) और राष्ट्रीय सुरक्षा अधिनियम, 1980 (NSA):**

a) CrPC की धारा 91 और 92 पुलिस को दस्तावेजों या संचार रिकॉर्ड को मंगवाने की शक्ति देती है।

b) NSA सरकार को निवारक निरोध (Preventive Detention) की शक्ति देता है, जो अक्सर गहन निगरानी के साथ जुड़ी होती है।

- **गैरकानूनी गतिविधियाँ (रोकथाम) अधिनियम, 1967 (UAPA):**

a) आतंकवाद विरोधी इस कानून के तहत सुरक्षा एजेंसियों को असाधारण शक्तियाँ प्राप्त हैं। UAPA के तहत संदिग्धों की डिजिटल और भौतिक निगरानी के लिए मानक प्रक्रियाओं को अक्सर दरकिनार किया जा सकता है, जिससे यह निजता के लिए एक गंभीर चुनौती बन जाता है।

3.3. निगरानी करने वाली एजेंसियाँ और उनकी शक्तियाँ:- भारत में कई एजेंसियाँ निगरानी गतिविधियों में शामिल हैं, जो गृह मंत्रालय (MHA) के समन्वय में कार्य करती हैं: * खुफिया एजेंसियाँ: इंटेलिजेंस ब्यूरो (IB) और रिसर्च एंड एनालिसिस विंग (R&AW)। ये एजेंसियाँ अक्सर विधायी जवाबदेही के बिना कार्य करती हैं क्योंकि इनका कोई विशिष्ट वैधानिक चार्टर नहीं है। * जाँच एजेंसियाँ: राष्ट्रीय जाँच एजेंसी (NIA), केंद्रीय अन्वेषण ब्यूरो (CBI), और प्रवर्तन निदेशालय (ED)। * अधिकृत एजेंसियाँ (2018 का आदेश): 2018 में गृह मंत्रालय ने 10 विशिष्ट एजेंसियों (जैसे IB, RAW, NCB, CBDT, आदि) को IT अधिनियम के तहत किसी भी कंप्यूटर डेटा को इंटरसेप्ट और डिक्रिप्ट करने के लिए अधिकृत किया। * शक्तियाँ: इन एजेंसियों के पास डेटा संग्रह, कॉल रिकॉर्ड (CDR) प्राप्त करने, और एन्क्रिप्टेड संचार तक पहुँचने की व्यापक शक्तियाँ हैं, जो अक्सर प्रशासनिक आदेशों के माध्यम से संचालित होती हैं।

3.4. न्यायिक समीक्षा और न्यायिक हस्तक्षेप:-

भारतीय न्यायपालिका ने निगरानी और निजता के बीच संतुलन बनाने में महत्वपूर्ण भूमिका निभाई है:

- **पीयूसीएल बनाम भारत संघ (PUCL vs. Union of India, 1996):** सर्वोच्च न्यायालय ने माना कि टेलीफोन टैपिंग निजता के अधिकार का उल्लंघन है। न्यायालय ने निगरानी के दुरुपयोग को रोकने के लिए "प्रक्रियात्मक सुरक्षा उपाय" (Procedural Safeguards) निर्धारित किए, जैसे कि केवल उच्च पदस्थ अधिकारियों द्वारा अनुमति और समीक्षा समितियों का गठन।
- **पुट्टुस्वामी निर्णय (2017):** जैसा कि पहले चर्चा की गई, इसने निजता को मौलिक अधिकार घोषित किया और निगरानी के लिए 'आनुपातिकता का परीक्षण' (Proportionality Test) अनिवार्य कर दिया। इसने मौजूदा निगरानी कानूनों की संवैधानिकता को चुनौती देने का एक नया आधार प्रदान किया।
- **पेगासस विवाद और सुप्रीम कोर्ट का रुख (2021):** स्पाइवेयर के माध्यम से कथित निगरानी के मामले में, सुप्रीम कोर्ट ने स्पष्ट किया कि "राष्ट्रीय सुरक्षा का हवाला देने मात्र से राज्य को खुली छूट (Free Pass) नहीं मिल जाती।" न्यायालय ने एक स्वतंत्र समिति नियुक्त की, जो निगरानी के मामलों में न्यायिक जवाबदेही की बढ़ती आवश्यकता को दर्शाती है।

3.5. मौजूदा ढाँचे में खामियाँ (Gaps in the Existing Framework)
यह खंड वर्तमान कानूनी व्यवस्था की गंभीर कमियों को उजागर करता है:

- **पारदर्शिता का अभाव (Opaque System):** निगरानी के आदेश गोपनीय होते हैं। नागरिकों को यह कभी पता नहीं चलता कि उन पर निगरानी रखी गई थी, जिससे वे इसे अदालत में चुनौती नहीं दे सकते।
- **स्वतंत्र निरीक्षण की कमी (Lack of Independent Oversight):** भारत में निगरानी की अनुमति 'कार्यपालिका' (Executive) ही देती है और उसकी समीक्षा भी 'कार्यपालिका' के ही अधिकारी (समीक्षा समिति) करते हैं। इसमें स्वतंत्र न्यायिक या संसदीय निरीक्षण का पूर्ण अभाव है।
- **व्यापक विवेक (Broad Discretion):** 'राष्ट्रीय सुरक्षा', 'सार्वजनिक व्यवस्था' और 'अपराध की जाँच' जैसे शब्दों का उपयोग इतना व्यापक है कि इनका उपयोग किसी भी प्रकार की असहमति को दबाने के लिए किया जा सकता है।
- **उत्तरदायित्व की कमी (Accountability Issues):** खुफिया एजेंसियों (IB, RAW) का कोई विधायी ढाँचा नहीं है, जिससे वे संसद के प्रति जवाबदेह नहीं हैं। दुरुपयोग के मामले में दंड के प्रावधान बहुत कमजोर हैं।
- **प्रभावी शिकायत निवारण तंत्र का अभाव:** यदि किसी व्यक्ति की निजता का अवैध रूप से उल्लंघन होता है, तो उसके पास कोई सरल या प्रभावी प्रशासनिक तंत्र नहीं है जहाँ वह शिकायत कर सके। उसे लंबी और महंगी न्यायिक प्रक्रिया का सहारा लेना पड़ता है।

4: डिजिटल युग में निगरानी प्रौद्योगिकियाँ और निजता पर उनका प्रभाव (Surveillance Technologies in the Digital Age and their Impact on Privacy):- यह अध्याय उन अत्याधुनिक तकनीकी उपकरणों का विश्लेषण करता है जिन्होंने निगरानी को "लक्षित" (Targeted) से "व्यापक" (Mass) में बदल दिया है। यह इस बात की पड़ताल करता है कि कैसे डेटा अब केवल एक संसाधन नहीं, बल्कि नियंत्रण का एक माध्यम बन गया है।

4.1. उन्नत निगरानी प्रौद्योगिकियाँ (Advanced Surveillance Technologies)
कृत्रिम बुद्धिमत्ता (AI) और मशीन लर्निंग (ML): AI अब केवल डेटा एकत्र नहीं करता, बल्कि उसका विश्लेषण और भविष्यवाणी भी करता है। 'प्रेडिक्टिव पुलिसिंग' (Predictive Policing) जैसे एल्गोरिदम यह अनुमान लगाने की कोशिश करते हैं कि अपराध कहाँ या किसके द्वारा किया जा सकता है। यह मानवीय हस्तक्षेप को कम करता है लेकिन तकनीकी निर्णय लेने की शक्ति को बढ़ाता है।
फेशियल रिकॉग्निशन तकनीक (Facial Recognition Technology - FRT): यह तकनीक सार्वजनिक स्थानों पर लगे सीसीटीवी कैमरों को 'स्मार्ट' बनाती है। बिना किसी की अनुमति के, भीड़ में से किसी की पहचान करना, उसके आने-जाने के रास्तों को ट्रैक करना अब संभव है। यह गुमनामी (Anonymity) के अधिकार को पूरी तरह समाप्त कर देता है।
बड़े डेटा (Big Data) और मेटाडेटा विश्लेषण: करोड़ों लोगों के डिजिटल फुटप्रिंट्स (कॉल, संदेश, सर्च हिस्ट्री) का विश्लेषण करके 'पैटर्न' पहचाने जाते हैं। मेटाडेटा (किसने, कब, कहाँ बात की) सामग्री से भी अधिक खतरनाक हो सकता है क्योंकि यह व्यक्ति के पूरे जीवन का खाका खींच देता है।
इंटरनेट ऑफ थिंग्स (IoT): स्मार्ट वॉच, स्मार्ट होम डिवाइस (जैसे एलेक्सा), और जुड़े हुए उपकरण लगातार डेटा भेजते हैं। हमारे निजी स्थानों (घरों) के अंदर की गतिविधियाँ अब डिजिटल रिकॉर्ड का हिस्सा हैं।
सोशल मीडिया और OSINT (Open-Source Intelligence): सरकारें अब सोशल मीडिया प्लेटफॉर्म्स की निगरानी के लिए विशेष 'सोशल मीडिया लैब' का उपयोग करती हैं। सार्वजनिक रूप से उपलब्ध जानकारी (OSINT) को एकत्र करके व्यक्तियों की राजनीतिक विचारधारा और संबंधों का विश्लेषण किया जाता है।
स्थान ट्रैकिंग (Location Tracking): जीपीएस और सेल-टॉवर ट्राइएंगुलेशन के माध्यम से राज्य यह जान सकता है कि कोई नागरिक किसी विशेष समय पर कहाँ था, वह किस विरोध प्रदर्शन में शामिल हुआ या वह किन लोगों से मिला।

4.2. निजता पर प्रभाव (Impact on Privacy)
मास सर्विलांस और 'चिलिंग इफेक्ट' (Chilling Effect): जब नागरिकों को पता होता है कि उन पर लगातार नज़र रखी जा रही है, तो वे अपनी वैध गतिविधियों (जैसे सरकार की आलोचना या विरोध) को कम कर देते हैं। यह आत्म-सेंसरशिप स्वतंत्र अभिव्यक्ति और लोकतंत्र के लिए घातक है।
प्रोफाइलिंग और एल्गोरिथम पूर्वाग्रह (Algorithmic Bias): निगरानी उपकरण अक्सर पूर्वाग्रह से ग्रस्त होते हैं। यदि डेटा पक्षपातपूर्ण है, तो AI विशिष्ट समुदायों, धर्मों या जातियों को "संदिग्ध" के रूप में चिह्नित कर सकता है, जिससे व्यवस्थागत भेदभाव पैदा होता है।
डी-एनॉनिमाइजेशन (De-anonymization): डेटा एकत्रीकरण इतना शक्तिशाली है कि अलग-अलग अनाम

(Anonymous) डेटासेट को मिलाकर किसी गुमनाम व्यक्ति की वास्तविक पहचान उजागर की जा सकती है। अब डिजिटल दुनिया में 'गुमनाम' रहना लगभग असंभव है।

सहमत की अवधारणा का क्षरण (Erosion of Consent): डिजिटल युग में "सहमति" अक्सर एक औपचारिकता बनकर रह गई है। उपयोगकर्ता अक्सर जटिल 'नियम और शर्तों' को समझे बिना सहमति देते हैं, और राज्य अक्सर राष्ट्रीय सुरक्षा के नाम पर सहमति की आवश्यकता को ही समाप्त कर देता है।

4.3. वैश्विक उदाहरण: उपयोग और दुरुपयोग (Global Examples)

चीन (व्यापक निगरानी का मॉडल): चीन का 'सोशल क्रेडिट सिस्टम' और शिनजियांग प्रांत में उइगरों पर फेशियल रिकॉग्निशन और बायोमेट्रिक्स के माध्यम से की जा रही निगरानी "हाई-टेक अधिनायकवाद" (High-tech authoritarianism) का सबसे प्रमुख उदाहरण है।

पश्चिमी देशों में चिंताएँ (USA/Europe):

- एडवर्ड स्नोडेन के खुलासे (NSA का PRISM प्रोग्राम) ने दिखाया कि कैसे अमेरिका जैसे लोकतंत्र भी बड़े पैमाने पर वैश्विक निगरानी में शामिल थे।
- इसके जवाब में, यूरोपीय संघ (EU) ने GDPR जैसे कड़े कानून बनाए हैं और कई देशों (जैसे बेल्जियम, इटली के कुछ शहर) ने सार्वजनिक स्थानों पर फेशियल रिकॉग्निशन पर प्रतिबंध या रोक लगा दी है।

पेगासस (Pegasus) और स्पाइवेयर का उदय: यह दिखाता है कि कैसे निजी कंपनियों द्वारा बनाए गए सैन्य-ग्रेड सॉफ्टवेयर का उपयोग सरकारों द्वारा पत्रकारों और कार्यकर्ताओं के खिलाफ किया जा रहा है, जिससे वैश्विक स्तर पर साइबर-निगरानी का एक नया संकट पैदा हो गया है।

5: तुलनात्मक विश्लेषण: अंतरराष्ट्रीय सर्वोत्तम अभ्यास और भारत के लिए सबक (Comparative Analysis: International Best Practices and Lessons for India):-यह अध्याय वैश्विक स्तर पर प्रचलित कानूनी ढाँचों का विश्लेषण करता है और यह जाँचता है कि भारत उनके सफल प्रयोगों से क्या सीख सकता है।

5.1. यूरोपीय संघ (European Union): निजता का 'स्वर्ण मानक'

- GDPR (General Data Protection Regulation): यह दुनिया का सबसे सख्त डेटा संरक्षण कानून है। यह नागरिकों को उनके डेटा पर पूर्ण नियंत्रण देता है (जैसे 'भूल जाने का अधिकार') और उल्लंघन पर भारी जुर्माने का प्रावधान करता है।
- न्यायिक निरीक्षण (CJEU): यूरोपीय संघ के न्यायालय (Court of Justice of the EU) ने 'श्रेम्स I और II' (Schrems I & II) जैसे ऐतिहासिक निर्णयों में स्पष्ट किया कि बड़े पैमाने पर (Bulk) और अंधाधुंध निगरानी अवैध है।
- डेटा संरक्षण प्राधिकरण (DPAs): प्रत्येक सदस्य देश में स्वतंत्र निकाय होते हैं जो यह सुनिश्चित करते हैं कि सरकारी एजेंसियां भी नियमों का पालन करें।
- भारत के लिए सबक: निगरानी केवल "अत्यंत आवश्यक" (Strict Necessity) और "आनुपातिक" (Proportional) होनी चाहिए।

5.2. संयुक्त राज्य अमेरिका (United States): न्यायिक वारंट और संवैधानिक सुरक्षा

- चौथा संशोधन (Fourth Amendment): अमेरिकी संविधान का यह संशोधन नागरिकों को "अनुचित तलाशी और जब्ती" (Unreasonable searches and seizures) से बचाता है। डिजिटल युग में इसकी व्याख्या डिजिटल डेटा तक विस्तारित की गई है।
- FISA और FISA कोर्ट: विदेश खुफिया निगरानी अधिनियम (FISA) के तहत, विदेशी जासूसी के लिए भी सरकार को एक गुप्त 'FISA कोर्ट' से अनुमति लेनी होती है। यह भारत के 'कार्यपालिका-केवल' मॉडल के विपरीत एक न्यायिक परत जोड़ता है।
- देशभक्ति अधिनियम (Patriot Act) से स्वतंत्रता अधिनियम (Freedom Act) तक: 9/11 के बाद लागू 'Patriot Act' की व्यापक आलोचना हुई। इसके बाद 'USA Freedom Act' (2015) के माध्यम से मेटाडेटा के थोक संग्रह (Bulk Collection) पर रोक लगाई गई, जो लोकतांत्रिक सुधार का उदाहरण है।
- भारत के लिए सबक: निगरानी के आदेशों के लिए किसी प्रकार का न्यायिक पूर्व-अनुमोदन (Judicial Pre-approval) आवश्यक है।

5.3. यूनाइटेड किंगडम (United Kingdom): 'डबल लॉक' प्रणाली

- जांच शक्तियाँ अधिनियम, 2016 (Investigatory Powers Act): हालाँकि इसे 'स्नूपर्स चार्टर' (Snooper's Charter) कहा जाता है और इसकी आलोचना भी होती है, लेकिन इसमें एक अनूठा 'डबल लॉक' (Double Lock) सिस्टम है।

- स्वतंत्र न्यायिक कमिश्नर (IPCO): ब्रिटेन में केवल मंत्री (Secretary of State) का आदेश काफी नहीं है; उस आदेश को एक स्वतंत्र न्यायिक आयुक्त (Judicial Commissioner) द्वारा अनुमोदित किया जाना अनिवार्य है।
- भारत के लिए सबक: "डबल लॉक" मॉडल भारत के लिए सबसे उपयुक्त हो सकता है, जहाँ गृह सचिव के आदेश की समीक्षा किसी सेवानिवृत्त न्यायाधीश या स्वतंत्र नियामक द्वारा की जाए।

5.4. तुलनात्मक अंतर्दृष्टि और भारत के लिए प्रासंगिकता

इस खंड में हम यह विश्लेषण करेंगे कि भारत को इन मॉडलों से क्या अपनाना चाहिए:

1. स्वतंत्रता बनाम सुरक्षा का संतुलन: भारत को चीन के "राज्य-सर्वोपरि" मॉडल के बजाय यूरोपीय संघ के "मानवाधिकार-केंद्रित" मॉडल की ओर झुकना चाहिए।
2. कार्यकारी विवेक को सीमित करना: भारत में वर्तमान में गृह सचिव ही निगरानी की अनुमति देते हैं और वही इसकी समीक्षा करते हैं। अंतरराष्ट्रीय उदाहरण बताते हैं कि यह "हितों का टकराव" (Conflict of Interest) है।
3. संसदीय निरीक्षण: अमेरिका और ब्रिटेन की तरह, भारत में भी खुफिया एजेंसियों (IB, RAW) के कामकाज की निगरानी के लिए एक 'संसदीय स्थायी समिति' होनी चाहिए।
4. तकनीकी मानक और ऑडिट: केवल कानूनी नहीं, बल्कि तकनीकी ऑडिट भी अनिवार्य होना चाहिए ताकि यह सुनिश्चित हो सके कि एकत्र किया गया डेटा सुरक्षित है और उसका उपयोग केवल उसी उद्देश्य के लिए हो रहा है जिसके लिए वह लिया गया था।

6: भारत के लिए एक नवीन नियामक ढाँचे का प्रस्ताव (Proposing a Novel Regulatory Framework for India)

6.1. सिद्धांतों का पुनर्गठन: डिजिटल युग के लिए पुट्टुस्वामी का विस्तार

- पुट्टुस्वामी मामले (2017) में सुप्रीम कोर्ट ने निजता के जो 9 आयाम बताए थे, उन्हें डिजिटल संदर्भ में पुनर्गठित करने की आवश्यकता है।
- नया सिद्धांत: "डिजिटल स्वायत्तता" (Digital Autonomy) और "एल्गोरिथम जवाबदेही" (Algorithmic Accountability)। यह केवल डेटा की सुरक्षा नहीं, बल्कि उस डेटा से होने वाले निर्णयों की सुरक्षा के बारे में भी है।

6.2. एक स्वतंत्र निगरानी प्राधिकरण (Independent Surveillance Authority - ISA) का निर्माण

संरचना: इसमें केवल कार्यपालिका (IAS अधिकारी) नहीं, बल्कि एक त्रिपक्षीय बोर्ड होना चाहिए:

1. **न्यायिक**: सेवानिवृत्त न्यायाधीश (कानूनी वैधता के लिए)।
2. **तकनीकी:** साइबर सुरक्षा और AI विशेषज्ञ (तकनीकी ऑडिट के लिए)।
3. **नागरिक समाज:** प्रख्यात मानवाधिकार कार्यकर्ता या शिक्षाविद (जनहित के लिए)।

शक्तियाँ: इसे जासूसी के आदेशों को रद्द करने, अवैध निगरानी के लिए जुर्माना लगाने और सुरक्षा एजेंसियों के सर्वर का औचक निरीक्षण करने का अधिकार होना चाहिए।

6.3. सख्त आनुपातिकता और आवश्यकता परीक्षण (The 'Proportionality' Standard)

पूर्व-अधिकृत न्यायिक वारंट: वर्तमान में गृह सचिव आदेश देते हैं। प्रस्ताव यह होना चाहिए कि बिना किसी उच्च न्यायालय के न्यायाधीश या विशेष रूप से नियुक्त 'निगरानी न्यायाधीश' के वारंट के कोई भी व्यक्तिगत निगरानी शुरू न हो। * न्यूनतम हस्तक्षेप: सरकार को यह साबित करना होगा कि निगरानी ही एकमात्र रास्ता है और कोई दूसरा कम हस्तक्षेपकारी साधन (जैसे सामान्य पूछताछ) उपलब्ध नहीं है।

डेटा प्रतिधारण (Retention): निगरानी से एकत्र डेटा को एक निश्चित अवधि (जैसे 90 दिन) के बाद स्वतः नष्ट कर दिया जाना चाहिए, जब तक कि वह अदालत में सबूत न बन जाए।

6.4. पारदर्शिता और जवाबदेही:

'अंधेरे' से 'प्रकाश' की ओर * सार्वजनिक रिपोर्टिंग: प्रतिवर्ष सरकार संसद में एक रिपोर्ट पेश करे (जैसे अमेरिका में होता है) जिसमें बताया जाए कि कुल कितने वारंट जारी किए गए, कितने सफल रहे और कितने रद्द हुए। (बिना राष्ट्रीय सुरक्षा के गुप्त ऑपरेशनों का खुलासा किए)।

क्षतिपूर्ति: यदि किसी नागरिक की अवैध रूप से निगरानी की गई है, तो उसे राज्य द्वारा हर्जाना मिलना चाहिए और दोषी अधिकारी को दंडित किया जाना चाहिए।

6.5. DPDP Act, 2023 के साथ एकीकरण: 'छूट' को सीमित करना धारा 17 का संशोधन: वर्तमान DPDP कानून सरकार को व्यापक छूट देता है। प्रस्ताव यह होना चाहिए कि 'राष्ट्रीय सुरक्षा' के नाम पर मिली यह छूट "पूर्ण" (Absolute) नहीं बल्कि "सशर्त" (Qualified) होनी चाहिए।

प्राइवेसी बाय डिज़ाइन: निगरानी प्रणालियों को बनाते समय ही उनमें ऐसे फिल्टर होने चाहिए जो गैर-जरूरी

डेटा को एकत्र ही न करें।

6.6. तकनीकी नैतिकता और AI दिशानिर्देश

स्वतंत्र ऑडिट: फेशियल रिकॉग्निशन (FRT) जैसे उपकरणों का उपयोग करने से पहले उनका 'प्राइवेसी इम्पैक्ट असेसमेंट' (PIA) अनिवार्य हो।

एल्गोरिथम पूर्वाग्रह: यह सुनिश्चित करना कि AI किसी विशेष समुदाय या विचारधारा को प्रोफाइल (Profile) न करे।

6.7. संसदीय निरीक्षण (Parliamentary Oversight) भारत में Intelligence and Security Committee (ISC) जैसी संसदीय समिति बनाई जानी चाहिए, जिसके पास खुफिया एजेंसियों के बजट और नीतियों की समीक्षा करने की शक्ति हो, जैसा कि ब्रिटेन और ऑस्ट्रेलिया में होता है।

7: निष्कर्ष और भविष्य की दिशाएँ (Conclusion and Future Directions)

7.1. प्रमुख शोध निष्कर्षों का सारांश (Summary of Findings)

- **कानूनी अंतराल**: शोध यह सिद्ध करता है कि भारत के वर्तमान निगरानी कानून (जैसे 1885 का टेलीग्राफ अधिनियम) डिजिटल युग की चुनौतियों (जैसे पेगासस, मेटाडेटा विश्लेषण) के लिए अपर्याप्त हैं।
- **संवैधानिक संघर्ष:** पुट्टुस्वामी निर्णय ने निजता को मौलिक अधिकार तो बना दिया, लेकिन ज़मीनी स्तर पर निगरानी की प्रक्रिया अभी भी काफी हद तक अपारदर्शी और कार्यकारी नियंत्रण में है।
- **संस्थागत कमी:** स्वतंत्र न्यायिक या विधायी निरीक्षण की अनुपस्थिति भारत के निगरानी तंत्र की सबसे बड़ी कमजोरी है।

7.2. प्रस्तावित नवीन नियामक ढाँचे का महत्व और संभावित प्रभाव

- **विश्वास की बहाली:** आपके द्वारा प्रस्तावित 'स्वतंत्र निगरानी प्राधिकरण' (ISA) से नागरिकों और राज्य के बीच डिजिटल विश्वास (Digital Trust) बढ़ेगा।
- **वैश्विक प्रतिष्ठा:** एक मजबूत ढांचा भारत को 'डेटा-सुरक्षित' राष्ट्र (Data-Secure Nation) के रूप में स्थापित करेगा, जिससे अंतरराष्ट्रीय व्यापार और निवेश में मदद मिलेगी।
- **निवारक प्रभाव:** न्यायिक वारंट की आवश्यकता सरकारी अधिकारियों द्वारा सत्ता के दुरुपयोग को कम करेगी।

7.3. नीतिगत सिफारिशें और कानून निर्माताओं के लिए निहितार्थ

- **निगरानी सुधार विधेयक:** संसद को एक समर्पित 'निगरानी सुधार अधिनियम' लाना चाहिए जो तकनीकी बारीकियों को समझे।
- **DPDP अधिनियम में संशोधन:** सरकारी छूट (Exemptions) को "अपरिहार्य परिस्थितियों" तक सीमित किया जाना चाहिए और उनके लिए भी समय-सीमा तय होनी चाहिए।
- **क्षमता निर्माण:** न्यायपालिका और कानून प्रवर्तन एजेंसियों को डिजिटल फोरेंसिक और निजता कानूनों के प्रति संवेदनशील और प्रशिक्षित किया जाना चाहिए।

7.4. भविष्य के लिए सुझाव

- **उभरती तकनीकें:** शोध के अगले चरण में क्वांटम कंप्यूटिंग (Quantum Computing) और जेनरेटिव एआई (GenAI) द्वारा निजता के उल्लंघन की संभावनाओं का अध्ययन किया जाना चाहिए।
- **सार्वजनिक जागरूकता:** 'डिजिटल साक्षरता' और 'निजता के अधिकार' के प्रति जन-जागरूकता अभियानों के प्रभाव का मूल्यांकन।
- **वैश्विक सहयोग:** एक 'अंतरराष्ट्रीय निगरानी संधि' (Global Surveillance Treaty) की आवश्यकता पर शोध, ताकि सीमा पार डेटा की निगरानी को विनियमित किया जा सके।

7.5. अंतिम विचार: सुरक्षा और स्वतंत्रता का स्थायी संतुलन

- **निष्कर्ष:** राष्ट्रीय सुरक्षा और व्यक्तिगत स्वतंत्रता एक-दूसरे के विरोधी नहीं, बल्कि पूरक हैं। एक असुरक्षित नागरिक स्वतंत्र नहीं हो सकता, और बिना निजता के सुरक्षा केवल दमन (Oppression) है।

"लोकतंत्र अंधेरे में नहीं मरता, बल्कि निरंतर निगरानी के साये में मरता है।" भारत को अपनी सुरक्षा के लिए अपनी लोकतांत्रिक आत्मा—स्वतंत्रता—का त्याग करने की आवश्यकता नहीं है। तकनीकी प्रगति को संवैधानिक मूल्यों के अधीन होना चाहिए, न कि उनके ऊपर।

संदर्भ ग्रंथ सूची (Bibliography)

1. कानूनी दस्तावेज (Legal Documents: Acts & Rules)
भारतीय साक्ष्य अधिनियम, 1872 (और नए भारतीय साक्ष्य अधिनियम, 2023 के प्रासंगिक प्रावधान)।
भारतीय टेलीग्राफ अधिनियम, 1885 (धारा 5(2))।

सूचना प्रौद्योगिकी अधिनियम, 2000 (विशेष रूप से धारा 66, 69 और 69A)।
सूचना प्रौद्योगिकी (मध्यवर्ती दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021।
डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (DPDP Act), 2023।
यूरोपीय संघ जनरल डेटा प्रोटेक्शन रेगुलेशन (EU GDPR), 2016।
अमेरिकी विदेशी खुफिया निगरानी अधिनियम (FISA), 1978।
2. न्यायिक निर्णय (Judicial Decisions)
भारत:
न्यायमूर्ति के.एस. पुट्टुस्वामी (सेवानिवृत्त) बनाम भारत संघ (2017) – (निजता का अधिकार निर्णय)।
पीयूसीएल (PUCL) बनाम भारत संघ (1997) – (फोन टैपिंग पर दिशा-निर्देश)।
खड़क सिंह बनाम उत्तर प्रदेश राज्य (1963) – (निगरानी और व्यक्तिगत स्वतंत्रता)।
विनीत कुमार बनाम सीबीआई (2019) – (निगरानी के लिए उचित प्रक्रिया की अनिवार्यता)।
अंतरराष्ट्रीय:
कारपेंटर बनाम संयुक्त राज्य अमेरिका (2018) – (डिजिटल स्थान डेटा की सुरक्षा)।
डिजिटल राइट्स आयरलैंड बनाम संचार मंत्री (यूरोपीय न्यायालय, 2014) – (डेटा प्रतिधारण पर निर्णय)।
3. शैक्षणिक पुस्तकें और शोध पत्र (Academic Books & Journals)
Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. (PublicAffairs, 2019).
Lyon, David. Surveillance Society: Monitoring Everyday Life. (Open University Press).
Bhatia, Gautam. The Transformative Constitution: A Magisterial Essay on Rights and Equality in India. (HarperCollins, 2019).
Schneier, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. (W. W. Norton).
शोध पत्र: "Privacy in the Age of Big Data" - Harvard Law Review.
शोध पत्र: "National Security vs. Individual Privacy" - Indian Journal of Constitutional Law.
4. सरकारी रिपोर्टें और नीतिगत दस्तावेज (Govt. Reports & Policy Docs)
न्यायमूर्ति बी.एन. श्रीकृष्ण समिति की रिपोर्ट (2018): "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians"।
न्यायमूर्ति ए.पी. शाह समिति की रिपोर्ट (2012): "Report of the Group of Experts on Privacy"।
विधि आयोग (Law Commission of India): निगरानी और डेटा सुरक्षा पर विभिन्न प्रासंगिक रिपोर्टें।
संयुक्त संसदीय समिति (JPC) रिपोर्ट: व्यक्तिगत डेटा संरक्षण विधेयक पर समीक्षा।
5. थिंक-टैंक रिपोर्ट और नागरिक समाज विश्लेषण (Think-Tank & CSO Reports)
Internet Freedom Foundation (IFF): "Privacy and Surveillance Reports (India)"।
Software Freedom Law Centre (SFLC.in): "India's Surveillance State Analysis"।
Observer Research Foundation (ORF): "Digital Sovereignty and Privacy Papers"।
Amnesty International: "The Pegasus Project: Technical Lab Reports"।
6. समाचार लेख और संपादकीय (News Articles & Editorials)
The Hindu: "Editorial: The Price of Privacy" (विशिष्ट तिथि के साथ)।
The Indian Express: "Explained: How Surveillance Laws Work in India"।
LiveLaw / Bar and Bench: कानूनी विश्लेषण और अदालती कार्यवाहियों का विवर