Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 4; 2025; Page No. 338-342

Received: 19-04-2025
Accepted: 28-06-2025
Published: 29-07-2025

डिजिटल गिरफ्तारियाँ और निजता का अधिकार

[1]Monika Singh Thakur and [2]Dr. Sarvendra Kumar

[1]Research Scholar, Mahakaushal University, Jabalpur, Madhya Pradesh, India
[2]Professor, Mahakaushal University, Jabalpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.20110442

Corresponding Author: Monika Singh Thakur

सारांश

"डिजिटल अरेस्ट" एक नया घोटाला है, जिसमें पीड़ितों को तब तक घोटालेबाजों के साथ वीडियो कॉल पर रहने के लिए मजबूर किया जाता है, जब तक कि उनकी मांगें पूरी नहीं हो जातीं। घोटालेबाज अधिकारी बनकर वीडियो कॉल पर बेखबर नागरिकों से पैसे ऐंठते हैं। अपराधी झूठे कानूनी मामलों को उजागर न करने के बदले में पैसे ऐंठ रहे हैं। वर्णनात्मक और तुलनात्मक शोध डिजाइन पर आधारित इस अध्ययन का उद्देश्य डिजिटल गिरफ्तारी और गोपनीयता के अधिकार के बीच संबंधों को समझना और विभिन्न देशों में अपनाए गए संवैधानिक सुरक्षा उपायों की तुलना करना है। डिजिटल युग में, जबकि प्रौद्योगिकी ने सामाजिक, आर्थिक और प्रशासनिक प्रक्रियाओं को सरल और त्वरित कर दिया है, इसने व्यक्तिगत स्वतंत्रता और गोपनीयता के अधिकार के लिए नई चुनौतियां भी उत्पन्न की हैं। इस संदर्भ में, इस अध्ययन का उद्देश्य इन चुनौतियों को समझना और उन्हें संबोधित करने के लिए प्रभावी संवैधानिक उपायों का विश्लेषण करना है।

मूलशब्द: डिजिटल गिरफ्तारियाँ, निजता का अधिकार, घोटाला, गोपनीयता

प्रस्तावना

भारत में निगरानी के लिए एक जटिल विनियामक ढांचा है, जिसमें सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 और भारतीय टेलीग्राफ अधिनियम, 1885 जैसे अवरोधन और निगरानी को अधिकृत करने वाले कई क़ानून शामिल हैं, साथ ही कई नियम और नीतियाँ भी हैं जो व्यापक रूपरेखा को संहिताबद्ध करती हैं जिसके अंतर्गत राज्य और गैर-राज्य अभिनेता निगरानी कर सकते हैं। उदाहरण के लिए, आईटी अधिनियम, 2000 सूचना के 'अवरोधन, निगरानी या डिक्रिप्शन' को अधिकृत करता है, जिससे पता चलता है कि भारत प्रौद्योगिकियों की कानूनी चुनौती के प्रति जागरूक हो रहा है।

इसके अलावा, भारतीय राज्य ने विभिन्न प्रकार की डिजिटल निगरानी पर भरोसा किया है - आधार जैसे बायोमेट्रिक अभिलेखागार से लेकर सेंट्रल मॉनिटरिंग सिस्टम (सीएमएस), नेटवर्क ट्रैफ़िक विश्लेषण (नेत्रा) और नेशनल इंटेलिजेंस ग्रिड (नैटग्रिड) जैसे बड़े पैमाने पर डिजिटल निगरानी आर्किटेक्चर तक - सुरक्षा, शासन और प्रशासन के उद्देश्यों के लिए थोक में डेटा एकत्र करने, मिलान करने और संसाधित करने के लिए। फिर भी, इन प्राधिकरण तकनीकों ने, एक बार उपयोग में आने के बाद, गोपनीयता के डर को जन्म दिया है। आधार प्रणाली को ही लें, जो प्रत्येक भारतीय निवासी को एक विशिष्ट पहचानकर्ता प्रदान करने का प्रयास है, जिसने गोपनीयता और गोपनीयता के दुरुपयोग से संबंधित कई विवाद उत्पन्न किए हैं।

साहित्य की समीक्षा

अंग्रिजा चक्रवर्ती (2019) [2] पर ध्यान देता हैडेटा प्रोटेक्शन लॉज़ डीमिस्टीफाइड में व्यक्तिगत डेटा की गोपनीयता और सुरक्षा के साथ-साथ क्लाइंट गोपनीय डेटा के मुद्दों को संबोधित किया गया है, जो विशेष रूप से यूरोपीय संघ के सामान्य डेटा संरक्षण विनियमन, भारत में व्यक्तिगत डेटा संरक्षण पर न्यायमूर्ति बीएन श्रीकृष्ण समिति द्वारा प्रस्तुत भारतीय डेटा संरक्षण विधेयक 2018 के नए मसौदे और दुनिया भर में अन्य प्रमुख गोपनीयता और व्यक्तिगत डेटा संरक्षण से संबंधित विधायी विकासों द्वारा सामने लाए गए हैं। पुस्तक का उद्देश्य कानून की प्रयोज्यता, डेटा

स्वामित्व, डेटा हैंडलिंग, डेटा सुरक्षा, डेटा विषय व्यक्ति के अधिकार और कानून के कानूनी या परिचालन अनुपालन से जुड़े प्रतिबंधों के बारे में असंख्य सवालों के जवाब देना है; जो वैश्विक अभिसरण, नई सूचना प्रौद्योगिकियों, बदलते व्यापार मॉडल और प्रथाओं, विकसित सामाजिक मानदंडों और नए और लगातार बदलते कानून के बाद उत्पन्न हुए हैं। यह एक व्यापक गोपनीयता कार्यक्रम को प्रभावी ढंग से लागू करने के तरीकों पर भी चर्चा करता है जो सभी प्रकार के व्यक्तिगत डेटा को सुरक्षित और प्रबंधित करने में सहायता करेगा, विशेष रूप से कॉर्पोरेट क्षेत्र और गैर-लाभकारी क्षेत्रों के संदर्भ में।

जूली एम. रोबिलार्डा, तान्या एल. फेंगा, अरलो बी. स्पोर्ना, जेन-ऐ लिया, कोडी लोआ, मोनिका ता, रोलैंड नाडलर (2019) [3] लोकप्रिय डिजिटल स्टोर के माध्यम से उपलब्ध मानसिक स्वास्थ्य ऐप की गोपनीयता नीतियों और समझौते की शर्तों की उपलब्धता, पठनीयता और गोपनीयता से संबंधित सामग्री का आकलन करने के उद्देश्य पर एक अलग दृष्टिकोण के बारे में बात करता है। शोधकर्ता ने लोकप्रिय स्मार्ट फोन ऐप स्टोर की खोज की, जो ट्रैक और मूड कीवर्ड और उनके समानार्थी शब्दों के संयोजन का उपयोग कर रहे थे। उन्होंने समावेशन और बहिष्करण मानदंडों के लिए प्रत्येक खोज से पहले 100 ऐप का मूल्यांकन किया। ऐप्स का मूल्यांकन गोपनीयता नीति और समझौते की शर्तों की उपलब्धता के लिए किया गया था और यदि उपलब्ध हो, तो दस्तावेज़ों का मूल्यांकन सामग्री और पठनीयता दोनों के लिए किया गया था। परिणामों में शोधकर्ता ने प्रदर्शित किया कि अधिकांश ऐप के साथ सूचना संग्रह हो रहा है जो उपयोगकर्ताओं को उनके मानसिक स्वास्थ्य की स्थिति को ट्रैक करने की अनुमति देता है। प्रारंभिक नमूने में एकत्र किए गए अधिकांश ऐप में स्टोर द्वारा यह आवश्यकता होने के बावजूद गोपनीयता नीति और समझौते की शर्तें शामिल नहीं थीं। कार्य ने यह भी विश्लेषण किया कि मूल्यांकन की गई अधिकांश गोपनीयता नीति और समझौते की शर्तें पोस्ट-सेकेंडरी रीडिंग स्तर पर लिखी गई थीं और खुलासा करती हैं कि व्यापक डेटा संग्रह हो रहा था। साथ ही, निष्कर्षों ने मानसिक स्वास्थ्य ऐप से जुड़ी सहमति, पारदर्शिता और डेटा साझाकरण के बारे में चिंताएँ जताईं और मोबाइल ऐप वातावरण में बेहतर विनियमन के महत्व पर प्रकाश डाला।

बर्नडेट कामलीटनर और विंस मिशेल (2019) [3] इस बारे में बात की है कि कैसे हर कोई दूसरों के बारे में व्यक्तिगत जानकारी रखता है। प्रत्येक व्यक्ति की गोपनीयता गंभीर रूप से कई अभिनेताओं के परस्पर क्रिया पर निर्भर करती है। प्रौद्योगिकी एकीकरण के युग में, डेटा सुरक्षा की यह अन्योन्याश्रयता गोपनीयता के लिए एक बड़ा खतरा बन रही है। वर्तमान विनियमन बहुकारक स्थितियों के बजाय दो पक्षों के बीच सूचना के आदान-प्रदान पर ध्यान केंद्रित करता है। शोधकर्ता इस बात पर प्रकाश डालता है कि यूरोपीय संघ के जनरल डेटा प्रोटेक्शन रेगुलेशन द्वारा चित्रित वर्तमान नीतिगत अपर्याप्तता को इस घटना की गहरी समझ के माध्यम से कैसे दूर किया जा सकता है। विशेष रूप से, लेखक अन्योन्याश्रित उल्लंघनों को समझाने के लिए एक नया घटना संबंधी ढांचा प्रस्तुत करता है। यह ढांचा संपत्ति और गोपनीयता के बीच समानताएं बनाने का भी प्रयास करता है और सुझाव देता है कि अन्योन्याश्रित सहकर्मी संरक्षण के लिए तीन पदानुक्रमित कदम, "3 आर" को समझना, पहचानना और सम्मान करना आवश्यक है। जबकि हस्तक्षेपों की पहली तीन श्रेणियां संबंधित 3आर से उत्पन्न होने वाले मुद्दों को संबोधित करती हैं, लेखक विशेष रूप से हस्तक्षेपों की चौथी श्रेणी की वकालत करते हैं जो क्रांतिकारी विकल्प प्रस्तावित करते हैं जो गोपनीयता संरक्षण की जिम्मेदारियों को उपभोक्ताओं से दूर कर देते हैं।

राहुल मथान (2018) [4] पुस्तक में हमारे निजी स्थान से संबंधित है। लेखक ने गोपनीयता की बदलती धारणाओं को शुरुआती समय से लेकर यू.के., यू.एस. और भारत में ऐतिहासिक मामलों के माध्यम से इसके विकास तक दर्शाया है। इस प्रक्रिया में, उन्होंने उस तरीके की फिर से कल्पना की है जिस तरह से हमें आज गोपनीयता के बारे में सोचना चाहिए अगर हमें आधुनिक डेटा प्रौद्योगिकियों का पूरा लाभ उठाना है, और उनके संभावित नुकसानों के बारे में इतना जुनूनी न होने के लिए आगाह किया है कि हम अपने कानूनों को इस तरह से डिजाइन करें कि हम उनसे बिल्कुल भी लाभ न उठा सकें।

ऋषभ बेली, स्मृति परशीरा, फैज़ा रहमान, रेणुका साने (2018) [5] भारत में पांच लोकप्रिय ऑनलाइन सेवाओं की गोपनीयता नीतियों की गुणवत्ता का मूल्यांकन पहुँच और पठनीयता के दृष्टिकोण से किया गया है। लेखकों ने सवालों के जवाब खोजने की कोशिश की जैसे नीतियों में विशिष्ट, स्पष्ट और स्पष्ट प्रावधान हैं जो खुद को आसान समझ में आते हैं, साथ ही कॉलेज के छात्रों के बीच शोध किया गया ताकि यह मूल्यांकन किया जा सके कि उपयोगकर्ता आमतौर पर उस चीज़ को कितना समझते हैं जिसके लिए वे साइन अप कर रहे हैं। लेखकों ने पाया कि अध्ययन की गई नीतियां खराब तरीके से तैयार की गई हैं, और अक्सर अपेक्षित गोपनीयता प्रकटीकरण के बॉक्स अनुपालन की जांच करने के रूप में कार्य करती प्रतीत होती हैं। उत्तरदाताओं ने उन नीतियों पर सबसे खराब प्रदर्शन किया जिनमें सबसे अधिक अनिर्दिष्ट शर्तें थीं और जो नीतियां लंबी थीं। काम में यह भी पाया गया कि उत्तरदाता तीसरे पक्ष, सहयोगी और व्यावसायिक भागीदार जैसे शब्दों को समझने में भी असमर्थ थे।

गोपनीयता और गोपनीयता का अधिकार

सुरक्षा और संरक्षण के अधिकार की अवधारणा जटिल है और इसे विभिन्न संदर्भों में विभिन्न तरीकों से व्याख्यायित किया गया है। एक सीधी उपयोगिता अवधारणा होने के बजाय, गोपनीयता एक जटिल विचार है जो केवल परिभाषा से अधिक विचार करने योग्य है। गोपनीयता की कोई स्पष्ट और सार्वभौमिक रूप से स्वीकृत कानूनी या दार्शनिक परिभाषा नहीं है।

"सुरक्षा" की व्युत्पत्ति लैटिन शब्द PRIVATUS से हुई है, जिसका अर्थ है "बाकी से अलग" या किसी चीज़ से वंचित। "PRIVO" से व्युत्पन्न, जिसका अर्थ है वंचित करना, गोपनीयता किसी व्यक्ति या समूह की अपने बारे में जानकारी छिपाने और, परिणामस्वरूप, उस जानकारी को दूसरों से छिपाने की क्षमता है।

गोपनीयता कोई प्रदत्त अधिकार नहीं है, बल्कि यह एक अंतर्निहित और स्वाभाविक अधिकार है। यह प्रदान नहीं किया जाता है, बल्कि पहले से ही मौजूद है। इसमें किसी व्यक्ति या व्यक्ति की अपने जीवन के कुछ पहलुओं को बिना किसी बाध्यकारी कारण के निजी रखने की इच्छा का सम्मान करना शामिल है।

ओल्मस्टेड बनाम यू.एस. के मामले में न्यायाधीश थॉमस कूली ने गोपनीयता की एक मौलिक परिभाषा प्रदान की, इसे अकेले रहने के अधिकार के रूप में संदर्भित किया। गोपनीयता के उल्लंघन को किसी व्यक्ति की व्यक्तिगत गतिविधियों में एक अनुचित हस्तक्षेप के रूप में देखा जाता है, जो टोर्ट कानून और कभी-कभी संवैधानिक कानून के तहत महत्वपूर्ण है। भारत में, गोपनीयता के अधिकार को अक्सर अकेले रहने के अधिकार के अर्थ में समझा जाता है। गोबिंद बनाम मध्य प्रदेश राज्य के मामले ने इस बात पर

जोर दिया कि जबकि व्यक्तियों को अकेले रहने का अधिकार है, उनकी स्वायत्तता समाज के साथ उनके संबंधों से प्रभावित होती है, जो स्वतंत्रता और स्वतंत्र विकल्प के बारे में सवाल उठा सकती है।
निजता के अधिकार को मौलिक मानव अधिकार के रूप में परिभाषित किया जा सकता है जो किसी व्यक्ति की स्वायत्तता की रक्षा करता है और उसकी व्यक्तिगत जानकारी पर नियंत्रण रखता है, तथा उसके निजी जीवन में अनुचित हस्तक्षेप को रोकता है। इस अवधारणा में यह विचार शामिल है कि व्यक्तियों को अपने जीवन, विचारों और गतिविधियों के कुछ पहलुओं को गोपनीय रखने और सरकार तथा अन्य संस्थाओं सहित दूसरों की पहुँच से परे रखने का अधिकार है।
निजता के अधिकार की एक महत्वपूर्ण अभिव्यक्ति सैमुअल वॉरेन और लुइस ब्रैंडिस द्वारा लिखे गए प्रभावशाली लेख "द राइट टू प्राइवेसी" में पाई जाती है। 1890 में हार्वर्ड लॉ रिव्यू में प्रकाशित, इस लेख को एक मौलिक कार्य माना जाता है जिसने संयुक्त राज्य अमेरिका में गोपनीयता कानून के विकास की नींव रखी। वॉरेन और ब्रैंडिस ने अकेले रहने के कानूनी अधिकार की मान्यता के लिए तर्क दिया, जिसमें कहा गया कि उभरती हुई प्रौद्योगिकियों और सामाजिक परिवर्तनों ने व्यक्तियों को उनके निजी मामलों में अनुचित प्रचार और घुसपैठ से बचाने की आवश्यकता पैदा की है।

भारत में निगरानी का ऐतिहासिक संदर्भ और विकास

भारत में निगरानी का इतिहास औपनिवेशिक काल से पहले, औपनिवेशिक काल से लेकर औपनिवेशिक काल के बाद तक की कहानी है, और यह ऐतिहासिक तकनीक और राजनीतिक समाजों के साथ सदियों से बदल रही है। निगरानी के विकास की यह ऐतिहासिक गाथा - सरल तकनीकों से लेकर परिष्कृत डिजिटल निगरानी तक - तकनीकों, कानूनों और प्रक्रियाओं की एक विशाल श्रृंखला को शामिल करती है जो राज्य की शक्ति, अधिकार और गोपनीयता के हितों के एक असहज मिश्रण को दर्शाती है।

प्रारंभिक निगरानी प्रथाएँ और उनके कानूनी आधार

स्वतंत्रता-पूर्व भारत में, निगरानी औपनिवेशिक शासन के अनुशासन और नियंत्रण दोनों के लिए एक उपकरण थी। ब्रिटिश राज ने उपनिवेश-विरोधी आंदोलनों को दबाने और नागरिक स्वतंत्रता के लिए किसी भी स्थान को नकारने की दिशा में आगे बढ़ने के लिए निगरानी को लागू करने के लिए कानून और उपाय लागू किए। 1885 का भारतीय टेलीग्राफ अधिनियम पहला कानून था जिसने 'सार्वजनिक सुरक्षा' के रखरखाव के लिए टेलीग्राफ संदेशों को रोकने के लिए सरकार के अधिकार को स्थापित किया, जो राज्य की निगरानी के लिए एक कानूनी आधार था।

राष्ट्रीय सुरक्षा के लिए निगरानी में स्वतंत्रता के बाद के विकास

निगरानी की औपनिवेशिक विरासत स्वतंत्र भारत की नव स्थापित लोकतांत्रिक सरकार को सौंप दी गई। स्वतंत्रता के बाद के शुरुआती वर्षों में औपनिवेशिक युग के कानूनों को नव-औपनिवेशिक काल के लिए बनाए रखा गया और संशोधित किया गया, जिसमें राष्ट्रीय सुरक्षा और क्षेत्रीय अखंडता पर व्यापक जोर दिया गया। इस संदर्भ में, 1885 का भारतीय टेलीग्राफ अधिनियम प्रमुख कानूनी साधन के रूप में काम करना जारी रखता है जिसके माध्यम से स्वतंत्र भारतीय सरकार ने 'राष्ट्रीय सुरक्षा के हित में' संचार की निगरानी और अवरोधन करने की मांग की है।

21वीं सदी में डिजिटल निगरानी का विकास

डिजिटल युग ने भारत में निगरानी के इतिहास में एक विशेष रूप से नाटकीय क्रांति ला दी है। सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की शुरुआत के साथ, कानून ने इलेक्ट्रॉनिक निगरानी की नई क्षमता और वास्तविकता को समझना शुरू कर दिया, जो इंटरनेट और मोबाइल टेलीफोन क्रांति द्वारा लाया गया था। आईटी अधिनियम ने 'इलेक्ट्रॉनिक रिकॉर्ड की कानूनी मान्यता', 'डिजिटल हस्ताक्षर और 'साइबर अपराध' जैसे क्षेत्रों को कवर किया, जो निगरानी के आधुनिक तरीकों के लिए मार्ग प्रशस्त करता है।

भारत में निगरानी को नियंत्रित करने वाला कानूनी ढांचा

भारत में निगरानी को सक्षम बनाने वाला न्यायिक ढांचा औपनिवेशिक युग के क़ानूनों और समकालीन विधानों का एक मिश्रण है, जो ऐतिहासिक न्यायिक मिसालों के साथ संयुक्त है, जिसके माध्यम से राज्य की सुरक्षा अनिवार्यताओं को व्यक्तिगत अधिकारों की पवित्रता के विरुद्ध संतुलित किया जाना चाहिए। ये तनाव बढ़ती आवृत्ति के साथ और तकनीकी और सांस्कृतिक परिवर्तन के साथ सामने आते हैं।

सरकारी छूट और निगरानी संबंधी चिंताएँ

इसके अलावा, अधिनियम में ऐसे प्रावधान हैं जो सरकार को कानून में उल्लिखित निगरानी-विरोधी सुरक्षा उपायों से भी स्पष्ट रूप से छूट देते हैं। कुछ अतिरिक्त अपवाद बनाए गए हैं और 'नियामक या पर्यवेक्षी निकायों' पर लागू होते हैं, और गोपनीयता अधिकार परिदृश्य के लिए महत्वपूर्ण, ऐसी छूट बनाने के लिए कोई स्पष्ट मानक नहीं हैं। भारत में संसाधित विदेशी डेटा से संबंधित प्रावधान की कमी सौदा विधेयक में जो प्रावधान थे, उनका अंतर्राष्ट्रीय सहयोग और विश्वास पर भी प्रभाव पड़ सकता है, विशेष रूप से जब यूरोपीय संघ जैसे पर्यवेक्षी प्राधिकरणों द्वारा पर्याप्तता निष्कर्ष की बात आती है।

डिजिटल गिरफ्तारी

साइबर खतरों के तेजी से विकसित हो रहे परिदृश्य में, डिजिटल गिरफ्तारी की अवधारणा एक नया खतरा बनकर सामने आई है। जालसाज कानून प्रवर्तन अधिकारियों का रूप धारण करके पीड़ितों को यह विश्वास दिलाते हैं कि उनके बैंक खाते, सिम कार्ड, आधार कार्ड या बैंक कार्ड का अवैध रूप से उपयोग किया गया है। वे पीड़ितों को पैसे देने के लिए मजबूर करते हैं। डिजिटल गिरफ्तारी में व्यक्तियों पर आभासी प्रतिबंध शामिल है। ये निलंबन खाते(ओं) और डिजिटल प्लेटफ़ॉर्म तक सीमित पहुँच से लेकर आगे की डिजिटल गतिविधियों को रोकने के उपायों को लागू करने या वीडियो कॉलिंग पर रोक लगाने या वीडियो कॉलिंग के ज़रिए निगरानी करने तक हो सकते हैं। डिजिटलीकरण के युग में जहाँ तकनीक तेज़ी से बढ़ रही है, अपराधियों द्वारा कई मौजूदा खामियों का उपयोग किया जा रहा है जिसने इस भयावह प्रवृत्ति को जन्म दिया है जिसे "डिजिटल गिरफ्तारी धोखाधड़ी" के रूप में जाना जाता है। इस घोटाले में, धोखेबाज़ पीड़ितों को बरगलाता है,

भविष्य का दृष्टिकोण

जहां तक इस बात का सवाल है कि क्या भारत निगरानी के भविष्य और सामान्य रूप से गोपनीयता के भविष्य के बारे में खुद को इस

अजीब स्थिति में पाता है, इसका उत्तर है: हां और नहीं। सबसे पहले, इसका उत्तर हां है क्योंकि लॉकडाउन के लागू होने के मामले में गड़बड़ी का कारण हमारी विफलता थी, जो एक त्वरित तकनीकी परिदृश्य के साथ-साथ एक समान रूप से त्वरित सामाजिक भूभाग को पूरी तरह से ध्यान में रखने में विफल रही। कर्फ्यू के बाद मानवीय मामलों में एआई और चेहरे की पहचान करने वाली तकनीकों का दखल लॉकडाउन से पहले का एक कृत्रिम बुद्धिमत्ता और चेहरे की पहचान शब्द है। भारत अब कर्फ्यू के बाद, लॉकडाउन के बाद का सामना कर रहा है। झूठ यह था कि निगरानी भारत को गुणात्मक रूप से अलग तरह की राष्ट्रीय सुरक्षा प्रदान करती है, लेकिन नहीं, क्योंकि आज, इन तकनीकों ने उन संभावनाओं को मूर्त रूप दिया है जो पहले से ही व्यक्तिगत गोपनीयता में बड़े पैमाने पर क्षरण के लिए एक असाधारण संरचनात्मक शर्त थी। अब यह सवाल नहीं है कि क्या भारत इन बिखरे हुए हितों को जोड़ने के लिए इस असंभव सुई को खोज पाएगा और अधिकारों की रक्षा करने वाली कानूनी, तकनीकी और निगरानी प्रणाली बनाएगा, या, क्या हम लड़खड़ाएंगे और एआई को बड़ी संख्या में भारतीयों की गोपनीयता को खत्म करने देंगे। अब सवाल यह नहीं है कि भारत कब प्रौद्योगिकी के साथ तालमेल बिठाएगा, बल्कि सवाल यह है कि हम ऐसा करेंगे।

उभरती हुई प्रौद्योगिकियाँ और निगरानी का भविष्य

- एआई: आर्टिफिशियल इंटेलिजेंस की सबसे बड़ी ताकतों में से एक इसकी बहुत बड़े डेटा सेट का विश्लेषण करने की क्षमता होगी; इसका उपयोग राष्ट्रीय सुरक्षा के लिए खतरों को कम करने के लिए किया जा सकता है, जिसमें आतंकवाद की भविष्यवाणी करने वाले पैटर्न की पहचान करने से लेकर संभावित साइबर हमलों के शुरुआती चरणों को रोकना शामिल है। लेकिन एआई-आधारित निगरानी गोपनीयता, भेदभाव और जवाबदेही के लिए महत्वपूर्ण मुद्दे भी उठाएगी, खासकर अगर एल्गोरिदम स्पष्ट या स्पष्ट मानदंडों के बिना अधिकारों के बारे में निर्धारण करते हैं।
- चेहरे की पहचान: भारत जैसे दुनिया भर में कानून प्रवर्तन और सुरक्षा एजेंसियों में चेहरे की पहचान करने वाले सॉफ़्टवेयर का उपयोग बढ़ रहा है। यह तकनीक अपराधियों की पहचान करने और संभावित रूप से अपराध होने से पहले उन्हें रोकने में बहुत मदद कर सकती है। हालाँकि, गोपनीयता के दृष्टिकोण से यह काफी विवादास्पद बना हुआ है। बड़े पैमाने पर निगरानी, लोगों की गलत पहचान और सार्वजनिक स्थानों पर गुमनामी के नुकसान की संभावना से जुड़े सवालों का समाधान किया जाना चाहिए।
- इंटरनेट ऑफ थिंग्स (IoT): IoT उपकरणों के प्रसार से लोगों के जीवन के सबसे अंतरंग स्थानों में निगरानी की क्षमता बढ़ जाती है, जिससे अत्यधिक जानकारी देने वाले डेटा एकत्रित हो जाते हैं, तथा इसके दुरुपयोग और लीक के विरुद्ध उच्चतम संभव सुरक्षा की आवश्यकता होती है।

भारत में संतुलित दृष्टिकोण की संभावनाएं

यदि भारत को निगरानी और गोपनीयता के नए क्षेत्र में सफल होना है, तो उसे कानूनी सुधारों, तकनीकी सुरक्षा उपायों और नवीन निरीक्षण तंत्रों को मिलाकर एक बहुस्तरीय दृष्टिकोण अपनाना होगा।

तकनीकी प्रगति के साथ तालमेल बनाए रखने के लिए विनियमन लागू करना अत्यंत महत्वपूर्ण है, जैसे कि कृत्रिम बुद्धि (AI) और चेहरे की पहचान के कुछ राज्यों द्वारा उपयोग पर स्पष्ट प्रतिबंध लगाना, डेटा सुरक्षा में सुधार करना, तथा निगरानी के उपयोग के संबंध में अधिक दृश्यता और जवाबदेही सृजित करना।

व्यक्तिगत गोपनीयता में सुधार करने वाली प्रौद्योगिकियों के लिए उदार सरकारी वित्त पोषण - उदाहरण के लिए, सामान्यीकृत गुमनामीकरण प्रौद्योगिकियां, एन्क्रिप्शन उपकरण, सामान्यीकृत 'डिजाइन द्वारा गोपनीयता' उपकरण - इन जोखिमों को काफी हद तक कम कर सकते हैं।

निगरानी शक्तियों पर जवाबदेही उपायों को बढ़ाना, चाहे न्यायिक, संसदीय या स्वतंत्र विनियामक निरीक्षण के माध्यम से हो, ताकि यह सुनिश्चित किया जा सके कि ऐसी शक्तियां कानून से जुड़े उद्देश्य की प्राप्ति के लिए आवश्यक तक ही सीमित हों, तथा व्यक्ति की गोपनीयता पर कोई अनुचित या गैरकानूनी आक्रमण न हो।

ज्ञान का आदान-प्रदान करने, साझा मानदंड और मानक विकसित करने तथा सीमा-पार डेटा-संरक्षण और निगरानी निरीक्षण में समन्वय स्थापित करने के लिए अंतर्राष्ट्रीय मंचों में भाग लेने से अंतर्राष्ट्रीय गोपनीयता और निगरानी विनियमन को बढ़ाने में मदद मिल सकती है।

निष्कर्ष

डिजिटल अरेस्ट का उदय धोखेबाज़ी और बलपूर्वक उपायों के माध्यम से लोगों की कमज़ोरियों का फ़ायदा उठाकर साइबर सुरक्षा के लिए एक उल्लेखनीय और अभिनव ख़तरा पेश करता है। नोएडा का मामला साइबर अपराधियों की हिम्मत और कौशल का एक प्रमुख उदाहरण है जो पीड़ितों को यह सोचने के लिए डर और झूठी जानकारी का इस्तेमाल करते हैं कि उन्हें कठोर कानूनी नतीजों का सामना करने और बड़ी मात्रा में पैसे लेने का ख़तरा है। इस बढ़ते साइबर अपराध से निपटने के लिए, लोगों को साइबर सुरक्षा के मामले में सक्रिय और सतर्क रुख अपनाने की ज़रूरत है। साइबर हाइजीन तकनीकें, जैसे कि दो-कारक प्रमाणीकरण और बार-बार पासवर्ड बदलना, अवांछित पहुँच की संभावना को कम करने के लिए आवश्यक हैं। महत्वपूर्ण सावधानियों में फ़िशिंग प्रयासों के बारे में जागरूक होना, विश्वसनीय एंटीवायरस सॉफ़्टवेयर के साथ डिवाइस की सुरक्षा करना और गोपनीयता बढ़ाने के लिए वर्चुअल प्राइवेट नेटवर्क (VPN) का उपयोग करना शामिल है। साइबर अपराधी और धोखेबाज़ अक्सर लोगों को हेरफेर करने और साइबर अपराध और वित्तीय धोखाधड़ी के क्षेत्र में अवैध लाभ के लिए उनकी कमज़ोरियों का फायदा उठाने के लिए एक शक्तिशाली उपकरण के रूप में डर का उपयोग करते हैं। डिजिटल गिरफ्तारी के धूर्त खतरे से खुद को बचाने के लिए, नेटिज़ेंस को सामूहिक ज्ञान, शिक्षित प्रथाओं और मजबूत साइबर सुरक्षा उपायों के साथ लगातार बदलते साइबर खतरे के परिदृश्य को पार करना होगा।

संदर्भ

1. स्वामीनाथन मीरा, अरिंद्रजीत बसु, निगरानी और डेटा संरक्षण: गोपनीयता और डिजिटल सुरक्षा के लिए खतरे, द सेंटर फॉर इंटरनेट एंड सोसाइटीज़, 2020.
2. अंगिरिजा चक्रवर्ती. डेटा संरक्षण कानून का रहस्य उजागर ओक ब्रिज पब्लिशिंग प्राइवेट लिमिटेड, प्रथम संस्करण, अक्टूबर, 2019.
3. जूली एम रोबिलार्डा, तान्या एल फेंगा, अर्लो बी स्पोर्ना, जेन-ऐ लाया, कोडी लोआ, मोनिका ताआ. रोलैंड नाडलर्ब: मानसिक

स्वास्थ्य ऐप्स की गोपनीयता नीतियों और समझौतों की शर्तों की उपलब्धता, पठनीयता और सामग्री, एल्सेवियर, 2019.
4. बर्नडेट कामलीटनर, विंस मिशेल, आपका डेटा मेरा डेटा है: परस्पर निर्भर गोपनीयता उल्लंघन को संबोधित करने के लिए एक रूपरेखा, जर्नल ऑफ पब्लिक पॉलिसी एंड मार्केटिंग राहुल मथन, गोपनीयता 3.0: हमारे डेटा-संचालित भविष्य को अनलॉक करना (हार्पर कॉलिन्स, 2018). 2019;38(4):433-450.
5. ऋषभ बेली स्मृति पर शीराफ़ैज़राहमान रेणुका साने, गोपनीयता नीतियों में प्रकटीकरण: क्या "नोटिस और सहमति" काम करती है?, नेशनल इंस्टीट्यूट ऑफ पब्लिक फाइनेंस एंड पॉलिसी एनआईपीएफपी वर्किंग पेपर सीरीज़ नंबर 2018, 246,.
6. क्रिस्टन ओ'लफलिन, मार्था नियरी, एलिजाबेथ सी. एडकिंस बी, स्टीफन एम. शूएलर, अवसाद के लिए मोबाइल ऐप्स की डेटा सुरक्षा और गोपनीयता नीतियों की समीक्षा, एल्सेवियर बी.वी., 2018.
7. अरका अध्ययन, भारत में मोबाइल ऐप्स और वेबसाइटों की डेटा गोपनीयता की स्थिति, 2018.
8. स्पायरोस ई. पॉलीकलास, व्यक्तिगत डेटा गोपनीयता के लिए सामान्य डेटा सुरक्षा विनियमन का आकलन: क्या ऐप्स डाउनलोड करने के लिए "इसे लें या छोड़ दें" दृष्टिकोण का अंत हो गया है? सोशल मीडिया प्रौद्योगिकी, संचार और सूचना विज्ञान, विनियमन पर सातवां अंतर्राष्ट्रीय सम्मेलन।
9. नेटवर्क और सूचना सुरक्षा के लिए यूरोपीय संघ एजेंसी (ENISA), मोबाइल अनुप्रयोगों में गोपनीयता और डेटा संरक्षण, ऐप विकास पारिस्थितिकी तंत्र और GDPR के तकनीकी कार्यान्वयन पर एक अध्ययन, 2017.
10. एफटीसी स्टाफ रिपोर्ट, मोबाइल गोपनीयता प्रकटीकरण निर्माण: पारदर्शिता के माध्यम से विश्वास, 2013.