ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 8, Issue 5,May 2018 Impact Factor 5.132 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

डिजिटल युग में तकनीकी निगरानी और गोपनीयता का संकट

नवीन कुमार

असिस्टेंट प्रोफेसर (समाजशास्त्र)

काशी नरेश राजकीय स्नातकोतर महाविद्यालय , ज्ञानपुर भदोहीसार

डिजिटल युग ने मानव जीवन के हर पहलू को क्रांति के पथ पर अग्रसर किया है। जहाँ एक ओर इसने संचार, व्यापार, शिक्षा और स्वास्थ्य जैसे क्षेत्रों में अभूतपूर्व प्रगति लाई है, वहीं दूसरी ओर इसने तकनीकी निगरानी और व्यक्तिगत गोपनीयता के बीच एक गंभीर संकट भी खड़ा कर दिया है। आज, हमारा अधिकांश जीवन ऑनलाइन है, और हर क्लिक, हर खोज, हर खरीदारी हमारे डिजिटल पदचिह्न छोड़ जाती है, जिसका उपयोग हमें ट्रैक करने और निगरानी करने के लिए किया जा सकता है। तकनीकी निगरानी का विस्तार विभिन्न रूपों में हुआ है। सरकारों द्वारा राष्ट्रीय सुरक्षा के नाम पर व्यापक निगरानी कार्यक्रम चलाए जाते हैं, जिसमें टेलीफोन कॉल, ईमेल और इंटरनेट गतिविधियों की निगरानी शामिल है। कॉर्पोरेट जगत में, डेटा ब्रोकर्स और विज्ञापन कंपनियाँ हमारे ऑनलाइन व्यवहार का गहन विश्लेषण करती हैं ताकि लक्षित विज्ञापन दिखाए जा सकें और उत्पादों को बढ़ावा दिया जा सके। स्मार्टफोन, स्मार्ट होम डिवाइस और इंटरनेट ऑफ थिंग्स उपकरण लगातार डेटा एकत्र कर रहे हैं, जो हमारी आदतों, स्थानों और यहां तक कि हमारे स्वास्थ्य के बारे में भी जानकारी प्रदान करते हैं। सोशल मीडिया प्लेटफॉर्म पर हमारी व्यक्तिगत जानकारी का विशाल भंडार होता है, जिसका उपयोग अक्सर हमारी सहमति के बिना या हमारी जानकारी के बिना किया जाता है।

मुख्य शब्द

डिजिटल, युग, तकनीकी, निगरानी, गोपनीयता

भूमिका

आज के डिजिटल युग में सोशल मीडिया प्लेटफॉर्म हमारे जीवन का अभिन्न अंग बन गए हैं। संचार, सूचना के आदान-प्रदान और मनोरंजन के लिए ये मंच अत्यधिक शक्तिशाली उपकरण साबित हुए हैं। फेसबुक, इंस्टाग्राम, ट्विटर, लिंक्डइन और अब टिक टॉक जैसे प्लेटफॉर्म ने दुनिया को एक वैश्विक गांव में बदल दिया है, जहाँ लोग एक दूसरे से आसानी से जुड़ सकते हैं। हालाँकि, इन प्लेटफॉर्म की बढ़ती लोकप्रियता के साथ ही एक गंभीर चिंता भी उभरी है: हमारी व्यक्तिगत गोपनीयता का संकट।

सोशल मीडिया प्लेटफॉर्म मुख्य रूप से उपयोगकर्ता डेटा पर चलते हैं। हमारी पसंद, नापसंद, हमारी गतिविधियाँ, स्थान, और यहाँ तक कि हमारी भावनाओं को भी ये प्लेटफॉर्म लगातार ट्रैक और रिकॉर्ड करते हैं। यह डेटा विज्ञापनों को लक्षित करने, उपयोगकर्ता अनुभव को बेहतर बनाने और व्यावसायिक रणनीतियों को आकार देने के लिए उपयोग किया जाता है। कहने को तो, यह सब हमारी सेवा के लिए है, लेकिन इस प्रक्रिया में हमारी गोपनीयता अक्सर दांव पर लग जाती है।

गोपनीयता के संकट के कई आयाम हैं। सबसे पहले, डेटा सुरक्षा का मुद्दा है। बड़ी मात्रा में व्यक्तिगत डेटा एक जगह जमा होने से हैकर्स और दुर्भावनापूर्ण तत्वों के लिए यह एक आकर्षक लक्ष्य बन जाता है। डेटा उल्लंघनों की खबरें आए दिन सुनने को मिलती हैं, जिससे लाखों उपयोगकर्ताओं की संवेदनशील जानकारी खतरे में पड़ जाती है। पहचान की चोरी, धोखाधड़ी और ब्लैकमेल जैसी घटनाएं इन उल्लंघनों का सीधा परिणाम हो सकती हैं।

यह निगरानी समाज के लिए कुछ लाभ भी प्रदान करती है। अपराधों की रोकथाम और जाँच में तकनीकी निगरानी एक महत्वपूर्ण उपकरण साबित हो सकती है। आतंकवादी गतिविधियों का पता लगाने और उन्हें रोकने में भी यह सहायक होती है। स्वास्थ्य सेवा में, डेटा विश्लेषण से बीमारियों का

बेहतर ढंग से निदान और उपचार संभव हो सकता है। स्मार्ट शहरों में, ट्रैफिक प्रबंधन और सार्वजनिक सुरक्षा में सुधार के लिए निगरानी तकनीकों का उपयोग किया जा सकता है।

इन लाभों के साथ ही गोपनीयता का संकट भी गहराता जा रहा है। व्यक्तिगत गोपनीयता का अधिकार एक मौलिक मानव अधिकार है, जो व्यक्ति को अपनी जानकारी को नियंत्रित करने और यह तय करने की शक्ति देता है कि उसे कैसे एकत्र, उपयोग और साझा किया जाए। जब तकनीकी निगरानी इस अधिकार का हनन करती है, तो कई गंभीर समस्याएं उत्पन्न होती हैं। सबसे पहले, यह नागरिक स्वतंत्रता पर खतरा पैदा करती है। अगर लोगों को यह पता हो कि उनकी हर गतिविधि पर नज़र रखी जा रही है, तो वे अपनी राय व्यक्त करने या असहमति जताने में संकोच कर सकते हैं, जिससे अभिव्यक्ति की स्वतंत्रता और लोकतांत्रिक प्रक्रियाएँ कमजोर होती हैं।

डेटा उल्लंघनों और साइबर हमलों का खतरा बढ़ जाता है। जितनी अधिक जानकारी एकत्र की जाती है, उतनी ही अधिक संभावना होती है कि वह जानकारी गलत हाथों में पड़ जाए। व्यक्तिगत डेटा की चोरी पहचान की चोरी, वित्तीय धोखाधड़ी और अन्य प्रकार के शोषण का कारण बन सकती है। तीसरे, यह भेदभाव और प्रोफाइलिंग को बढ़ावा दे सकता है। एकत्र किए गए डेटा का उपयोग व्यक्तियों को उनके जाति, धर्म, लिंग या राजनीतिक झुकाव के आधार पर लक्षित करने या भेदभाव करने के लिए किया जा सकता है।

इस संकट का समाधान बहुआयामी दृष्टिकोण की मांग करता है। सबसे पहले, मजबूत डेटा संरक्षण कानूनों और नियमों की आवश्यकता है जो व्यक्तियों को अपनी जानकारी पर अधिक नियंत्रण दें। इसमें डेटा उपयोग के लिए स्पष्ट सहमति, डेटा पोर्टेबिलिटी का अधिकार और डेटा मिटाने का अधिकार शामिल होना चाहिए। भारत में डेटा संरक्षण विधेयक इस दिशा में एक महत्वपूर्ण कदम है, लेकिन इसके

प्रभावी कार्यान्वयन और निरंतर अद्यतन की आवश्यकता है।

तकनीकी कंपनियों को अपनी व्यावसायिक प्रथाओं में पारदर्शिता और जवाबदेही सुनिश्चित करनी चाहिए। उन्हें यह स्पष्ट करना चाहिए कि वे कौन सा डेटा एकत्र कर रहे हैं, इसका उपयोग कैसे कर रहे हैं और इसे किसके साथ साझा कर रहे हैं। उपयोगकर्ता-अनुकूल गोपनीयता सेटिंग्स और गोपनीयता-केंद्रित डिज़ाइन भी महत्वपूर्ण हैं।

साहित्य की समीक्षा

जनता में डिजिटल साक्षरता और जागरूकता बढ़ाना आवश्यक है। लोगों को अपने डिजिटल पदचिह्न के बारे में सूचित होना चाहिए और अपनी गोपनीयता की रक्षा के लिए आवश्यक कदम उठाने चाहिए, जैसे कि मजबूत पासवर्ड का उपयोग करना, गोपनीयता सेटिंग्स को समझना और संदिग्ध लिंक पर क्लिक न करना। [1]

कई बार, सोशल मीडिया कंपनियां तीसरे पक्ष के साथ उपयोगकर्ता डेटा साझा करती हैं, अक्सर हमारी पूरी जानकारी या सहमति के बिना। कैम्ब्रिज एनालिटिका घोटाला इसका एक ज्वलंत उदाहरण था, जहाँ लाखों फेसबुक उपयोगकर्ताओं के डेटा का उपयोग राजनीतिक अभियानों को प्रभावित करने के लिए किया गया था। यह दर्शाता है कि हमारा डेटा न केवल व्यावसायिक उद्देश्यों के लिए, बल्कि सामाजिक और राजनीतिक हेरफेर के लिए भी इस्तेमाल किया जा सकता है। [2]

एल्गोरिदम की भूमिका है। सोशल मीडिया प्लेटफॉर्म पर मौजूद एल्गोरिदम यह तय करते हैं कि हम क्या देखते हैं, किससे जुड़ते हैं, और किस तरह की जानकारी हमें मिलती है। ये एल्गोरिदम हमारी ऑनलाइन गतिविधियों के आधार पर हमारी डिजिटल प्रोफाइल बनाते हैं। [3]

समस्या तब उत्पन्न होती है जब ये प्रोफाइल बहुत विस्तृत और सटीक हो जाते हैं, जिससे हमारी डिजिटल स्वतंत्रता और स्वायत्तता पर सवाल उठता है। हमारी ऑनलाइन आदतों का लगातार विश्लेषण और हमें विशिष्ट सामग्री की पेशकश से, हमारे विचारों और व्यवहार को भी अप्रत्यक्ष रूप से प्रभावित किया जा सकता है। [4]

डिजिटल युग में तकनीकी निगरानी और गोपनीयता का संकट

आज के डिजिटल युग में, जहाँ हमारा जीवन इंटरनेट और तकनीक पर अत्यधिक निर्भर हो गया है, "साइबर हमलों का खतरा" एक गंभीर संकट बनकर उभरा है। व्यक्तिगत जानकारी से लेकर राष्ट्रीय सुरक्षा तक, सब कुछ डिजिटल नेटवर्क से जुड़ा है, और ऐसे में साइबर हमलावर लगातार नए और परिष्कृत तरीकों से प्रणालियों को भेदने का प्रयास कर रहे हैं। यह संकट व्यक्तियों, व्यवसायों और सरकारों के लिए बड़े पैमाने पर वित्तीय, गोपनीय और परिचालन संबंधी जोखिम पैदा करता है।

गोपनीयता के इस संकट का समाज पर व्यापक प्रभाव पड़ता है। यह विश्वास में कमी लाता है। जब उपयोगकर्ताओं को यह एहसास होता है कि उनकी गोपनीयता का सम्मान नहीं किया जा रहा है, तो वे इन प्लेटफॉर्म पर भरोसा करना बंद कर देते हैं। इससे अभिव्यक्ति की स्वतंत्रता भी प्रभावित हो सकती है, क्योंकि लोग अपनी बात कहने से पहले दो बार सोचने लगते हैं, इस डर से कि उनके डेटा का दुरुपयोग किया जा सकता है।

इस संकट से निपटने के लिए कई कदम उठाए जाने की आवश्यकता है। सबसे पहले, सरकारों को मजबूत डेटा सुरक्षा कानूनों और विनियमों को लागू करना चाहिए। यूरोपीय संघ का जीडीपीआर इसका एक अच्छा उदाहरण है, जो व्यक्तिगत डेटा के संग्रह, प्रसंस्करण और भंडारण पर सख्त नियम लागू

करता है। भारत में भी प्रस्तावित डेटा संरक्षण विधेयक इसी दिशा में एक महत्वपूर्ण कदम है।

सोशल मीडिया प्लेटफॉर्म को अपनी पारदर्शिता और जवाबदेही बढ़ानी होगी। उन्हें उपयोगकर्ताओं को यह स्पष्ट रूप से बताना होगा कि उनका डेटा कैसे एकत्र किया जाता है, उपयोग किया जाता है और साझा किया जाता है। उपयोगकर्ताओं को अपने डेटा पर अधिक नियंत्रण देने वाले विकल्प प्रदान किए जाने चाहिए। उपयोगकर्ताओं को भी अपनी डिजिटल साक्षरता बढ़ानी होगी। हमें अपनी गोपनीयता सेटिंग्स की समीक्षा करनी चाहिए, यह समझना चाहिए कि हम क्या साझा करते हैं, और अनावश्यक जानकारी साझा करने से बचना चाहिए। हमें सोशल मीडिया प्लेटफॉर्म की शर्तों और नीतियों को ध्यान से पढ़ना चाहिए, भले ही वे लंबी और जटिल क्यों न हों।

सोशल मीडिया प्लेटफॉर्म ने निस्संदेह हमारे संचार और कनेक्टिविटी में क्रांति ला दी है। हालांकि, यह क्रांति हमारी गोपनीयता की कीमत पर नहीं होनी चाहिए। सोशल मीडिया कंपनियों, सरकारों और उपयोगकर्ताओं को मिलकर काम करना होगा ताकि डिजिटल दुनिया में गोपनीयता के अधिकार का सम्मान हो सके। केवल तभी हम इन शक्तिशाली उपकरणों के लाभों का पूरी तरह से आनंद ले पाएंगे, बिना अपनी व्यक्तिगत स्वतंत्रता और सुरक्षा से समझौता किए।

मैलवेयर एक सामान्य शब्द है जिसमें वायरस, वर्म्स, ट्रोजन और रैनसमवेयर जैसे दुर्भावनापूर्ण सॉफ़्टवेयर शामिल होते हैं। रैनसमवेयर विशेष रूप से चिंताजनक है, क्योंकि यह सिस्टम को तब तक लॉक कर देता है जब तक हमलावर को फिरौती नहीं दी जाती। फ़िशिंग हमलों में धोखेबाज ईमेल या संदेशों का उपयोग करके उपयोगकर्ताओं को संवेदनशील जानकारी (जैसे पासवर्ड या बैंक विवरण) उजागर करने के लिए बरगलाया जाता है। डिनायल-ऑफ-सर्विस और डिस्ट्रीब्यूटेड डिनायल-ऑफ-सर्विस हमले किसी वेबसाइट या ऑनलाइन सेवा को अनुपलब्ध बनाने के लिए उस पर भारी मात्रा में

ट्रैफ़िक भेजकर उसे अधिभारित कर देते हैं। मैन-इन-द-मिडिल हमले में हमलावर दो संवाद करने वाले पक्षों के बीच खुद को स्थापित कर लेता है और उनके संचार को इंटरसेप्ट या संशोधित करता है। SQL इंजेक्शन हमले वेबसाइटों के डेटाबेस को निशाना बनाते हैं और हमलावरों को संवेदनशील डेटा तक पहुंचने या उसे संशोधित करने की अनुमति देते हैं।

इन साइबर हमलों के प्रभाव दूरगामी और विनाशकारी हो सकते हैं। व्यक्तियों के लिए, इसका अर्थ पहचान की चोरी, वित्तीय नुकसान, व्यक्तिगत डेटा का दुरुपयोग और मानसिक तनाव हो सकता है। व्यवसायों के लिए, साइबर हमले से भारी वित्तीय क्षति होती है, जिसमें डेटा उल्लंघन की लागत, परिचालन में रुकावट, राजस्व का नुकसान, कानूनी शुल्क और ब्रांड की प्रतिष्ठा को नुकसान शामिल है। उदाहरण के लिए, डेटा उल्लंघनों से ग्राहकों का विश्वास खत्म हो सकता है और कंपनियों को भारी नियामक जुर्माना भरना पड़ सकता है। सरकारों के लिए, साइबर हमले महत्वपूर्ण बुनियादी ढांचे (जैसे ऊर्जा ग्रिड और संचार नेटवर्क) को बाधित कर सकते हैं, राष्ट्रीय सुरक्षा को खतरे में डाल सकते हैं, गोपनीय जानकारी चुरा सकते हैं और यहां तक कि अंतर्राष्ट्रीय संबंधों को भी प्रभावित कर सकते हैं। साइबर युद्ध का खतरा, जिसमें राष्ट्र एक दूसरे के सिस्टम को निशाना बनाते हैं, एक बढ़ती हुई चिंता है।

संगठनों और सरकारों को भी साइबर सुरक्षा पर भारी निवेश करने की आवश्यकता है। इसमें मजबूत सुरक्षा प्रोटोकॉल लागू करना, नियमित रूप से भेद्यता आकलन और प्रवेश परीक्षण करना, कर्मचारियों को साइबर सुरक्षा प्रशिक्षण प्रदान करना, डेटा एन्क्रिप्शन का उपयोग करना और घटना प्रतिक्रिया योजनाएं विकसित करना शामिल है। आर्टिफिशियल इंटेलिजेंस और मशीन लर्निंग जैसी नई तकनीकों का उपयोग साइबर खतरों का पता लगाने और उनसे बचाव के लिए किया जा सकता है।

साइबर हमलों का खतरा आज के डिजिटल युग में एक अदम्य चुनौती है। यह एक ऐसा संकट है जिसके

लिए निरंतर सतर्कता, शिक्षा और सहयोग की आवश्यकता है। व्यक्तियों, व्यवसायों और सरकारों को मिलकर एक मजबूत साइबर सुरक्षा पारिस्थितिकी तंत्र बनाने के लिए काम करना होगा ताकि हम डिजिटल क्रांति के लाभों का सुरक्षित रूप से लाभ उठा सकें और इस बढ़ते संकट के विनाशकारी प्रभावों से खुद को बचा सकें। साइबर सुरक्षा केवल एक तकनीकी मुद्दा नहीं है, बल्कि यह हमारी सामूहिक सुरक्षा और भविष्य के लिए एक महत्वपूर्ण आवश्यकता है।

निष्कर्ष

डिजिटल युग में तकनीकी निगरानी और गोपनीयता का संकट एक जटिल चुनौती है। इसका समाधान केवल सरकारों या कंपनियों की जिम्मेदारी नहीं है, बल्कि यह हम सभी की सामूहिक जिम्मेदारी है। हमें प्रौद्योगिकी के लाभों का आनंद लेते हुए अपनी गोपनीयता के अधिकार की रक्षा के लिए जागरूक और सक्रिय रहना होगा, ताकि एक ऐसा डिजिटल भविष्य निर्मित किया जा सके जो सुरक्षित, स्वतंत्र और न्यायपूर्ण हो। सरकारों को राष्ट्रीय सुरक्षा और व्यक्तिगत गोपनीयता के बीच संतुलन स्थापित करने के लिए एक नैतिक और कानूनी ढाँचा विकसित करना होगा। निगरानी कार्यक्रमों को सख्त न्यायिक के तहत संचालित किया जाना चाहिए, और यह सुनिश्चित किया जाना चाहिए कि उनका उपयोग केवल वैध उद्देश्यों के लिए ही हो और गोपनीयता के अधिकार का अनावश्यक रूप से उल्लंघन न हो।

संदर्भ

1. डिजिटल निगरानी : एक परिचय, संपादक: डॉ. प्रभाकर झा और डॉ. राधिका झा (2015)
2. डिजिटल गोपनीयता , लेखक: डॉ. संजय कुमार (2014)
3. डिजिटल संकट, लेखक: डॉ. राकेश कुमार सिंह (2014)

4. डिजिटल शिक्षाशास्त्र: एक नया दृष्टिकोण, लेखक: डॉ. प्रभाकर झा (2015)

5. डिजिटल युग का महत्व, लेखक: डॉ. राधिका झा (2014)

6. डिजिटल तकनीक का उपयोग, लेखक: डॉ. संजय कुमार (2015)