SHIKSHA SAMVAD
International Journal of Multidisciplinary Research
ISSN: 2584-0983 (Online)
© Shiksha Samvad|Volume-03| Issue-02| December- 2025
Available online at: https://shikshasamvad.com/
DOI:- https://doi.org/10.64880/shikshasamvad.v3i2.7

डिजिटल युग में महिला गोपनीयता का संकट: डेटा सुरक्षा, स्वतंत्रता और सामाजिक दृष्टिकोण

डॉ श्वेता द्विवेदी

असिस्टेंट प्रोफेसर, समाजशास्त्र विभाग, रणवीर रणंजय स्नातकोत्तर महाविद्यालय अमेठी

email- dwivedishweta85@gmail.com

सारांश

डिजिटल परिवर्तन ने संचार, शिक्षा, रोजगार और सामाजिक जुड़ाव के क्षेत्र में व्यापक संभावनाएँ विकसित की हैं, लेकिन इसके साथ महिलाओं की डिजिटल गोपनीयता पर नए खतरे भी पैदा हुए हैं। सोशल मीडिया प्लेटफ़ॉर्म, डिजिटल पहचान प्रणालियाँ, ऑनलाइन वित्तीय सेवाएँ और निगरानी तकनीकें जहाँ महिलाओं को आत्मनिर्भरता और अभिव्यक्ति की स्वतंत्रता देती हैं, वहीं साइबर स्टॉकिंग, डेटा चोरी, ऑनलाइन उत्पीड़न, डीपफेक और डिजिटल ट्रैकिंग जैसी समस्याएँ उनके लिए गंभीर जोखिम भी उत्पन्न करती हैं। शोध डिजिटल वातावरण में महिलाओं की निजता को प्रभावित करने वाले तकनीकी, कानूनी और सामाजिक आयामों का विश्लेषण करता है। अध्ययन से स्पष्ट होता है कि वर्तमान कानूनी ढाँचा मौजूद होने के बावजूद क्रियान्वयन की चुनौतियाँ, शिकायत प्रणाली की जटिलता और सामाजिक दृष्टिकोण की सीमाएँ महिलाओं को न्याय और सुरक्षा से दूर रखती हैं। डिजिटल सुरक्षा केवल तकनीकी आवश्यकता नहीं, बल्कि सामाजिक, नैतिक और लैंगिक न्याय का विषय भी है। इसलिए डिजिटल अधिकार, सशक्त कानूनी संरक्षण, साइबर साक्षरता और संवेदनशील व्यवहार परिवर्तन आवश्यक है, ताकि डिजिटल स्पेस महिलाओं के लिए सुरक्षित, समान और समावेशी बन सके।

मुख्य शब्द: डिजिटल गोपनीयता, महिला सशक्तिकरण, साइबर सुरक्षा, डेटा संरक्षण, ऑनलाइन उत्पीड़न।

प्रस्तावना

21वीं सदी की डिजिटल क्रांति ने संचार, शासन, शिक्षा, श्रम-बाज़ार और सामाजिक संपर्कों को पारंपरिक सीमाओं से आगे बढ़ाकर एक ऐसी वास्तविकता में परिवर्तित कर दिया है, जहाँ वास्तविक और आभासी जीवन अब अलग नहीं, बल्कि एकीकृत रूप में मौजूद हैं। इस दौर में व्यक्ति केवल भौतिक रूप से नहीं, बल्कि अपने डिजिटल स्वरूप में भी पहचाना जाता है। इसी कारण समाज अब "नेटवर्केड वास्तविकता" की दिशा में विकसित हो चुका है, जहाँ विचारों, व्यवहारों और सामाजिक संबंधों को डिजिटल डेटा के रूप में संग्रहित और प्रसारित किया जाता है।[1] इस संदर्भ में फ़ूको की *Surveillance Theory* एक महत्वपूर्ण दृष्टिकोण प्रस्तुत करती है। उनके अनुसार आधुनिक समाज एक ऐसी panoptic व्यवस्था में रूपांतरित हो चुका है जहाँ व्यक्ति निरंतर अदृश्य निगरानी के अधीन रहता है।[2] डिजिटल तकनीक ने इस विचार को और मजबूत रूप दिया है, जिसे समकालीन विचारक "Digital Panopticon"[3] नाम देते हैं—एक ऐसी निगरानी प्रणाली, जो दिखाई नहीं देती, परंतु उसका प्रभाव अत्यधिक शक्तिशाली होता है।

इस ढांचे में महिला एक सामाजिक श्रेणी के रूप में सबसे अधिक प्रभावित समूह है क्योंकि डिजिटल स्पेस में उसकी उपस्थिति केवल डेटा तक सीमित नहीं, बल्कि उसकी पहचान, प्रतिष्ठा, शरीर और स्वतंत्रता से जुड़ी होती है।[4]

भारत जैसे समाज में, जहाँ लैंगिक असमानता ऐतिहासिक और सांस्कृतिक स्तर पर स्थापित है, डिजिटल भागीदारी ने जहाँ अवसरों के नए द्वार खोले हैं, वहीं जोखिमों का दायरा भी बढ़ाया है। National Family Health Survey (NFHS-5, 2021) के अनुसार केवल लगभग 33% महिलाएँ ही इंटरनेट का उपयोग कर पाती हैं, और उनमें से 67% ने स्वीकार किया कि ऑनलाइन गतिविधियों के दौरान उन्हें गोपनीयता उल्लंघन, साइबर स्टॉकिंग, डेटा दुरुपयोग, अश्लील संदेश, मॉर्फ्ड इमेज या ब्लैकमेल जैसे खतरों का डर बना रहता है।[5] यह स्थिति स्पष्ट करती है कि डिजिटल सशक्तिकरण और डिजिटल सुरक्षा के बीच गंभीर असमानता मौजूद है।

महिलाओं की डिजिटल पहचान पारंपरिक पहचान से कहीं अधिक जटिल है, क्योंकि यह केवल तकनीकी सुविधा नहीं, बल्कि अभिव्यक्ति की स्वतंत्रता, सामाजिक सहभागिता, आर्थिक आत्मनिर्भरता और व्यक्तिगत निर्णय लेने के अधिकार से जुड़ी हुई है।[6] अतः डिजिटल गोपनीयता का संकट केवल तकनीकी विफलता नहीं, बल्कि पितृसत्ता, लैंगिक भेदभाव और सत्ता संरचनाओं से निर्मित एक व्यापक सामाजिक-सांस्कृतिक समस्या है।[7]

डिजिटल युग में महिला की गोपनीयता का प्रश्न इसलिए विशेष महत्व रखता है क्योंकि तकनीक ने निजी और सार्वजनिक क्षेत्रों की सीमाओं को धुंधला कर दिया है। आज उसकी तस्वीरें, लोकेशन, बातचीत, बैंकिंग जानकारी, बायोमेट्रिक डेटा और सामाजिक नेटवर्क—सब निगरानी योग्य और दुरुपयोग योग्य डिजिटल संसाधन बन चुके हैं।[8]

- **साहित्य-समीक्षा**

Sherry Turkle (2011) की पुस्तक Alone Together बताती है कि तकनीक मानव संबंधों, गोपनीयता और भावनात्मक सुरक्षा को प्रभावित करती है तथा डिजिटल युग में पहचान जटिल होती है।[9]

Judy Wajcman (2004) ने TechnoFeminism में बताया कि तकनीक लैंगिक तटस्थ नहीं, बल्कि पितृसत्तात्मक संरचनाओं से प्रभावित होती है, जिससे महिलाओं का डिजिटल अनुभव असमान होता है।[10]

Zuboff (2019) की Surveillance Capitalism में डिजिटल प्लेटफ़ॉर्म द्वारा डेटा संग्रह, निगरानी और नियंत्रण की प्रक्रिया को उजागर किया गया है, विशेषकर महिलाओं के संदर्भ में।[11]

Bauman (2013) की Liquid Surveillance बताती है कि निरंतर निगरानी डिजिटल समाज का सामान्य व्यवहार बन चुका है, जिससे व्यक्तिगत स्वतंत्रता और गोपनीयता प्रभावित होती है।[12]

Nussbaum (2011) के Capabilities Approach में महिलाओं की स्वतंत्रता, गरिमा और डिजिटल भागीदारी को मानव अधिकारों की नजर से विश्लेषित किया गया है।[13]

David Lyon (2015) की Surveillance Studies में बताया गया है कि डिजिटल निगरानी सामाजिक असमानता को मजबूत करती है और महिलाओं पर इसका प्रभाव अधिक गंभीर होता है।[14]

- **शोध का उद्देश्य**

1. डिजिटल युग में महिला गोपनीयता संकट के उभरते रूपों की पहचान करना।
2. डेटा सुरक्षा और व्यक्तिगत स्वतंत्रता के संदर्भ में कानूनी तथा नीतिगत अवस्थाओं की समीक्षा करना।
3. समाज में मौजूद पितृसत्तात्मक रवैये का महिलाओं की डिजिटल स्वतंत्रता पर प्रभाव समझना।

4. केस स्टडी और द्वितीयक डेटा के आधार पर संबंधित समस्याओं और निवारक उपायों का विश्लेषण करना।

➢ **शोध प्रविधि**

इस शोध में वर्णनात्मक एवं विश्लेषणात्मक शोध पद्धति अपनाई गई है। डेटा संग्रह के लिए प्राथमिक एवं द्वितीयक दोनों प्रकार के स्रोतों का उपयोग किया गया। प्राथमिक स्रोतों में केस स्टडी, समाचार विवरण, कानूनी दस्तावेज और डिजिटल अनुभवों की समीक्षा शामिल है। द्वितीयक स्रोतों के रूप में पुस्तकों, शोध-पत्रों, सरकारी रिपोर्टों और ऑनलाइन डेटाबेस का उपयोग किया गया। अध्ययन में सैद्धांतिक ढाँचे पर आधारित तुलनात्मक और गुणात्मक विश्लेषण किया गया।

➢ **सैद्धांतिक रूपरेखा**

डिजिटल युग में महिलाओं की गोपनीयता से जुड़े संकट को केवल तकनीकी दृष्टिकोण से समझ पाना संभव नहीं है। इसे समझने के लिए सामाजिक, सांस्कृतिक, राजनीतिक और लैंगिक संदर्भों पर आधारित विश्लेषण आवश्यक है। इसी उद्देश्य से इस शोध में विभिन्न प्रमुख सिद्धांतों को आधार बनाया गया है, जो न केवल डिजिटल व्यवहार को स्पष्ट करते हैं, बल्कि सत्ता संरचना, तकनीकी हस्तक्षेप और जोखिमों की प्रकृति को भी रेखांकित करते हैं।

Surveillance Theory: माइकल फ़ूको की ***Surveillance Theory*** आधुनिक समाज में शक्ति और निगरानी के संबंधों को समझाती है।[15] फ़ूको का तर्क है कि तकनीक केवल व्यक्ति के क्रियाकलापों पर नियंत्रण नहीं रखती, बल्कि उसकी चेतना को इस प्रकार ढाल देती है कि वह स्वयं को हमेशा निगरानी में अनुभव करता है। डिजिटल संदर्भ में यह विचार *algorithmic surveillance* और *data tracking* के रूप में दिखाई देता है, जहाँ महिला की डिजिटल गतिविधियाँ निरंतर रिकॉर्ड और विश्लेषण योग्य बन जाती हैं।[16]

Feminist Cyber Theory: Judy Wajcman द्वारा प्रस्तुत ***Feminist Cyber Theory*** है। यह सिद्धांत यह स्पष्ट करता है कि डिजिटल तकनीक लैंगिक रूप से निष्पक्ष नहीं होती, बल्कि यह उसी सामाजिक ढाँचे द्वारा निर्मित होती है जहाँ पितृसत्तात्मक मानदंड सदियों से विद्यमान हैं।[11] इस दृष्टिकोण से ऑनलाइन ट्रोलिंग, डीपफेक, उत्पीड़न और डिजिटल शोषण जैसी घटनाएँ तकनीक के माध्यम से दोहराया गया लैंगिक असमानता का ही रूप हैं।[17]

Technological Determinism: Marshall McLuhan का *Technological Determinism* है, जिसके अनुसार तकनीक केवल साधन नहीं, बल्कि एक ऐसी शक्ति है जो समाज के ढाँचों, व्यवहारों और संबंधों को पुनः परिभाषित करती है।[18] इस विचार के अनुसार डिजिटल तकनीक ने संचार की प्रकृति बदली है और इसके साथ ही गोपनीयता, प्रतिष्ठा और लैंगिक सुरक्षा की धारणाएँ भी बदल गई हैं।

Risk Society Theory: Ulrich Beck की *Risk Society Theory* यह संकेत देती है कि आधुनिक समाज नव-निर्मित जोखिमों के अधीन है—ऐसे जोखिम जिन्हें न देखा जा सकता है और न तत्काल रोक पाना संभव होता है।[19] साइबर ब्लैकमेल, डेटा चोरी, डीपफेक और वर्चुअल हिंसा इसी "निर्मित डिजिटल जोखिम" की श्रेणी में आते हैं।

डिजिटल गोपनीयता संकट के रूप: विश्लेषण

डिजिटल परिवेश में महिलाओं की सुरक्षा और स्वायत्तता निम्नलिखित जटिल चुनौतियों से प्रभावित होती है-

1. **साइबर स्टॉकिंग और ऑनलाइन उत्पीड़न:** ऑनलाइन स्पेस में उत्पीड़न डिजिटल हिंसा की सबसे व्यापक श्रेणी है, जो अपमानजनक टिप्पणियों, धमकियों, अवांछित संदेशों, ट्रोलिंग और गलत सूचना के प्रसार के रूप में प्रकट होती है। कई बार महिलाएँ केवल अपनी तस्वीर साझा करने, किसी सामाजिक विषय पर राय व्यक्त करने या सार्वजनिक रूप से सक्रिय होने भर से निशाना बन जाती हैं। साइबर स्टॉकिंग के मामलों में अपराधी महिला की लोकेशन, डिजिटल गतिविधि और सामाजिक संपर्कों पर लगातार नज़र रखता है। इस प्रकार का व्यवहार

पीड़ित के भीतर भय, आत्म-संदेह, सामाजिक दूरी और मानसिक तनाव को जन्म देता है। मॉर्फ्ड तस्वीरें, अवांछित वीडियो कॉल और धमकी भरे संदेश अक्सर महिला की आवाज़ और स्वतंत्रता को दबाने का माध्यम बनते हैं।

2. **डेटा चोरी और डिजिटल पहचान का जोखिम**: डिजिटल पहचान अब केवल बुनियादी जानकारी तक सीमित नहीं है, बल्कि इसमें बैंकिंग रिकॉर्ड, स्वास्थ्य डेटा, बायोमेट्रिक विवरण, निजी संचार और लोकेशन हिस्ट्री जैसी संवेदनशील जानकारियाँ सम्मिलित हैं। जैसे-जैसे शासन और सेवा तंत्र डिजिटल रूप ले रहे हैं, महिलाओं का डेटा साइबर अपराध के लिए एक महत्वपूर्ण संसाधन बन गया है। डिजिटल footprints वर्षों तक संग्रहीत रहते हैं, इसलिए चोरी किया गया डेटा लंबे समय तक दुरुपयोग किया जा सकता है। कई महिलाएँ फिशिंग लिंक, नकली मोबाइल ऐप्स या असुरक्षित वेबसाइटों के माध्यम से अनजाने में संवेदनशील जानकारी साझा कर देती हैं, जिससे उनकी डिजिटल सुरक्षा और अधिक कमजोर हो जाती है।
3. **डीपफेक और टेक्नो-यौन हिंसा-** कृत्रिम बुद्धिमत्ता आधारित डीपफेक तकनीक ने ऑनलाइन लैंगिक हिंसा को अत्यंत गंभीर और जटिल बना दिया है। किसी महिला की साधारण तस्वीर को बिना अनुमति अश्लील वीडियो या छवि में बदल देना न केवल पहचान और गरिमा पर हमला है, बल्कि यह मानसिक, सामाजिक और कानूनी संकट का रूप भी लेता है। ऐसे मामलों में पीड़िता को प्रतिष्ठा हानि, सामाजिक कलंक, ब्लैकमेल और अवसाद जैसी समस्याओं का सामना करना पड़ता है। इसके परिणामस्वरूप कई महिलाएँ डिजिटल माध्यमों से दूरी बनाने या स्वयं को सेंसर करने के लिए बाध्य हो जाती हैं।
4. **निजी संबंधों और परिवार के भीतर डिजिटल निगरानी**- डिजिटल गोपनीयता का उल्लंघन केवल बाहरी खतरों से नहीं होता, बल्कि यह परिवार, रिश्तों और सामाजिक संबंधों के भीतर भी प्रकट होता है। कई परिवारों में महिलाओं की चैट, कॉल सूची, पासवर्ड, लोकेशन और सोशल मीडिया गतिविधियों की निगरानी सुरक्षा या नैतिक जिम्मेदारी का रूप देकर आवश्यक बताई जाती है। प्रेम संबंधों और विवाह के संदर्भ में पासवर्ड साझा करना या डिवाइस चेक करना अक्सर विश्वास या प्रेम की कसौटी समझा जाता है। यह व्यवहार महिला की स्वायत्तता, गोपनीयता और निर्णय क्षमता को सीमित करता है और डिजिटल स्पेस को उसके लिए नियंत्रित और निगरानी-आधारित क्षेत्र में बदल देता है।

➢ **केस स्टडी (Case Studies)**

डिजिटल गोपनीयता संकट की वास्तविकता को समझने के लिए केवल सिद्धांत पर्याप्त नहीं, बल्कि उन ठोस उदाहरणों का विश्लेषण भी आवश्यक है जो इस समस्या के व्यावहारिक और मानवीय पहलुओं को उजागर करते हैं। केस स्टडी यह दर्शाती हैं कि डिजिटल खतरों की प्रकृति व्यक्तिगत संबंधों, तकनीकी अवसरों और सामाजिक विचारधाराओं से किस प्रकार गहराई से जुड़ी होती है। भारत में साइबर अपराधों से प्रभावित महिलाओं की संख्या निरंतर बढ़ रही है, और आश्चर्यजनक रूप से अधिकांश मामलों में अपराधी पीड़िता के सामाजिक दायरे के ही सदस्य होते हैं — जैसे मित्र, सहपाठी, रिश्तेदार या तकनीकी सेवा प्रदाता। निम्नलिखित अध्ययन डिजिटल निजता के व्यवस्थित उल्लंघन के स्वरूप को स्पष्ट करते हैं:

केस अध्ययन–1: डीपफेक तकनीक और सोशल मीडिया दुरुपयोग

सन् 2023 का एक चर्चित मामला दिल्ली से सामने आया, जहाँ 17 वर्षीय स्कूली छात्रा की इंस्टाग्राम प्रोफ़ाइल से तस्वीरें डाउनलोड कर उसके सहपाठियों ने एआई आधारित डीपफेक वीडियो तैयार किए और उन्हें विभिन्न सोशल मीडिया प्लेटफ़ॉर्म पर प्रसारित किया।[20] इस घटना के परिणामस्वरूप पीड़िता और उसके परिवार को गंभीर मानसिक, सामाजिक और भावनात्मक दबाव झेलना पड़ा।

इस मामले ने दो महत्वपूर्ण चिंताएँ उजागर कीं:

1. अपराधी अक्सर कोई अजनबी नहीं बल्कि सामाजिक संबंधों के भीतर के लोग होते हैं।

2. डीपफेक निर्माण के लिए उच्च स्तरीय तकनीकी कौशल की नहीं, बल्कि आसानी से उपलब्ध मोबाइल एप्लिकेशन की आवश्यकता होती है।

यद्यपि आरोपियों को गिरफ्तार किया गया, परंतु एक बार प्रसारित सामग्री को पूर्णतः हटाया नहीं जा सका — जो डिजिटल क्षेत्र में हानि की स्थायित्व प्रकृति को दर्शाता है।

केस अध्ययन–2: साइबर ब्लैकमेल और तकनीकी विश्वास का दुरुपयोग

मुंबई की 24 वर्षीय महिला ने अपने स्मार्टफ़ोन को मरम्मत हेतु एक मोबाइल रिपेयर दुकान पर दिया। बाद में उसे निजी तस्वीरों का उपयोग कर ब्लैकमेल किया जाने लगा। पुलिस जांच से खुलासा हुआ कि तकनीशियन ने 300 से अधिक महिलाओं के निजी डेटा को अपने पास संग्रहित कर रखा था और उनका दुरुपयोग कर रहा था।[21]

यह मामला तीन स्तरों की कमजोरियों को प्रदर्शित करता है:

- तकनीकी सेवा प्रदाताओं की नैतिक ज़िम्मेदारी का अभाव
- संस्थागत निगरानी और नियामक प्रावधानों की कमी
- विश्वास और गोपनीयता का गंभीर उल्लंघन

इस घटना के बाद साइबर सेल ने नियमों को सख़्त करने और रिपेयर दुकानों में डेटा सुरक्षा उपायों को अनिवार्य बनाने पर जोर दिया।

तुलनात्मक तालिका-1:

क्रम	केस अध्ययन	अपराध का स्वरूप	अपराधी की पहचान	तकनीकी माध्यम	मुख्य प्रभाव	निष्कर्ष / कार्यवाही
1	दिल्ली डीपफेक केस	एआई आधारित यौन उत्पीड़न	सहपाठी	Deepfake Apps	सामाजिक अपमान, मानसिक आघात	गिरफ्तारी, लेकिन सामग्री का शमन कठिन
2	मुंबई साइबर ब्लैकमेल केस	डेटा चोरी व ब्लैकमेल	मोबाइल टेक्नीशियन	डेटा एक्सट्रैक्शन टूल्स	भय, आर्थिक दबाव, डिजिटल अलगाव	आरोपी गिरफ्तार, जाँच जारी

विश्लेषणात्मक निष्कर्ष- इन केस स्टडी से प्राप्त मुख्य सार निम्न रूप में उभरता है:

- साइबर हिंसा का बड़ा हिस्सा परिचित लोगों द्वारा संचालित होता है, इसलिए "सुरक्षा" की पारंपरिक धारणाएँ डिजिटल स्पेस में अप्रासंगिक होती जा रही हैं।
- डिजिटल सहभागिता में वृद्धि के साथ ही महिलाओं के प्रति अपराध भी अधिक तकनीकी और छुपे हुए स्वरूप में सामने आ रहे हैं।
- कानूनी हस्तक्षेप होने पर भी डिजिटल अपराधों की क्षति को पूर्णतः समाप्त करना अत्यंत चुनौतीपूर्ण है।
- तकनीक का विकास तभी लाभकारी है जब उसके साथ सुरक्षा, नैतिकता और उत्तरदायित्व की संरचना समान गति से विकसित हो।

➢ **कानून और नीतिगत ढाँचा**

भारत में डिजिटल स्पेस में महिलाओं की सुरक्षा, गोपनीयता संरक्षण और ऑनलाइन समानता सुनिश्चित करने हेतु अनेक कानून, नीतियाँ और विनियम समय—समय पर लागू किए गए हैं। यद्यपि इन प्रावधानों का उद्देश्य महिलाओं को डिजिटल उत्पीड़न, डाटा दुरुपयोग, साइबर हिंसा और निजता के

उल्लंघन से बचाना है, फिर भी वास्तविक स्तर पर उनका प्रभाव सीमित दिखाई देता है, क्योंकि क्रियान्वयन, जागरूकता और संस्थागत संवेदनशीलता में अभी भी सुधार की आवश्यकता बनी हुई है।

सबसे प्रमुख आधार सूचना प्रौद्योगिकी अधिनियम (Information Technology Act, 2000) है, जो भारत में साइबर अपराधों को परिभाषित और नियंत्रित करने वाली प्राथमिक विधि है। इस अधिनियम के तहत सेक्शन 66E निजी जानकारी के अवैध संग्रह और प्रसार पर रोक लगाता है, जबकि सेक्शन 67 और 67A अश्लील सामग्री, नग्नता, आपत्तिजनक तस्वीरों और पोर्नोग्राफिक सामग्री के डिजिटल प्रसार से संबंधित अपराधों को नियंत्रित करते हैं। ये प्रावधान विशेष रूप से महिलाओं से जुड़े मामलों—जैसे मॉर्फिंग, डीपफेक वीडियो, गैर—सहमति आधारित फोटो साझा करना और ऑनलाइन ब्लैकमेलिंग—में प्रभावी भूमिका निभाते हैं।

इसके अलावा, भारतीय दंड संहिता (IPC) भी डिजिटल प्लेटफॉर्म पर महिलाओं के खिलाफ अपराधों को दंडनीय बनाती है। IPC की धारा 354D "साइबर स्टॉकिंग" यानी किसी महिला का लगातार डिजिटल पीछा करने, संदेश भेजने या ऑनलाइन निगरानी करने को अपराध घोषित करती है। इसी तरह, धारा 509 किसी महिला की गरिमा को ठेस पहुँचाने वाली भाषा, टिप्पणी, आवाज़ संदेश या डिजिटल कंटेंट को कानूनी दायरे में लाती है। इन प्रावधानों की मौजूदगी के बावजूद, व्यवहारिक स्तर पर पुलिस की तकनीकी क्षमता, डिजिटल साक्ष्य संकलन की दक्षता और पीड़ितों के प्रति संवेदनशील रवैये में कमी के कारण, कई मामलों में न्याय प्रक्रिया धीमी और थकाऊ हो जाती है।[22]

इसी संदर्भ में POSH Act (2013) का विस्तार भी उल्लेखनीय है। प्रारंभिक रूप से यह अधिनियम औपचारिक कार्यस्थलों पर होने वाले यौन उत्पीड़न को नियंत्रित करने के लिए बनाया गया था, लेकिन महामारी पश्चात वर्चुअल मीटिंग, ऑनलाइन वर्कस्पेस और दूरस्थ कार्य पद्धतियों के प्रचलन के कारण अब इसका दायरा ऑनलाइन उत्पीड़न और डिजिटल कार्यस्थल भी शामिल करता है।[23]

महिलाओं की डिजिटल पहचान, बायोमेट्रिक सूचना, व्यक्तिगत डेटा और ऑनलाइन ट्रैकिंग से जुड़े खतरों को देखते हुए वर्ष 2023 में लागू **Digital Personal Data Protection Act (DPDP Act, 2023)** इस क्षेत्र में एक महत्वपूर्ण मील का पत्थर माना जा रहा है। यह कानून सरकारी संस्थाओं, प्राइवेट कंपनियों, सोशल मीडिया प्लेटफ़ॉर्म और डेटा प्रोसेसरों पर यह बाध्यता डालता है कि किसी भी व्यक्ति—विशेषकर महिला—का डेटा उसकी स्पष्ट सहमति के बिना संग्रहित, संचित या साझा नहीं किया जा सकता। यह अधिनियम पारदर्शिता, डेटा संरक्षण, जवाबदेही और दुरुपयोग की स्थिति में दंड प्रणाली पर आधारित है।[24] हालाँकि इन सभी विधियों की उपस्थिति महत्वपूर्ण है, लेकिन इनके वास्तविक प्रभाव में कई बाधाएँ मौजूद हैं। साइबर विशेषज्ञों और प्रशिक्षित पुलिस कर्मियों की कमी, केस रजिस्ट्रेशन की जटिल प्रक्रिया, प्रमाण संकलन के तकनीकी चरण, तथा न्याय प्रणाली में लंबी प्रतीक्षा—ये सभी कारक कानून के प्रभाव को सीमित करते हैं। इसके अतिरिक्त, कई महिलाएँ डिजिटल अधिकारों, कानूनी प्रावधानों और शिकायत निवारण तंत्र से अनभिज्ञ रहती हैं, जिसके कारण बड़ी संख्या में मामले रिपोर्ट ही नहीं होते।

इसलिए यह आवश्यक है कि केवल कानून बनाना पर्याप्त नहीं, बल्कि उनके प्रभावी क्रियान्वयन, साइबर फॉरेंसिक अवसंरचना के विकास, राष्ट्रीय स्तर पर डिजिटल साक्षरता अभियान और तेज न्याय तंत्र की स्थापना भी समान रूप से प्राथमिकता प्राप्त करे। जब तक तकनीकी कौशल, कानूनी जागरूकता और सामाजिक दृष्टिकोण में सुधार नहीं होगा, तब तक महिलाओं की डिजिटल सुरक्षा केवल कानूनी दस्तावेजों तक सीमित रह जाएगी।[25]

तालिका-2: भारत में महिला डिजिटल सुरक्षा से संबंधित प्रमुख कानून

क्रम संख्या	कानून / धारा	उद्देश्य	लागू क्षेत्र
1	IT Act 2000	डिजिटल अपराधों पर नियंत्रण	सोशल मीडिया, डेटा चोरी, साइबर स्टॉकिंग
2	IPC 354D	साइबर स्टॉकिंग रोकना	मोबाइल, चैट, लोकेशन ट्रैकिंग

3	IPC 509	महिला की गरिमा का संरक्षण	ऑनलाइन गाली-गलौज, अभद्र संदेश
4	POSH Act	ऑनलाइन कार्यस्थल सुरक्षा	ईमेल, वर्चुअल मीटिंग, ऑफिस प्लेटफॉर्म
5	Digital Data Protection Act 2023	डेटा प्राइवेसी और डिजिटल अधिकार	आधार, भुगतान ऐप, सरकारी प्लेटफ़ॉर्म

Sources: Information Technology Act, 2000 (भारत का सूचना प्रौद्योगिकी अधिनियम, 2000)

सामाजिक दृष्टिकोण और लैंगिक परिप्रेक्ष्य: डिजिटल दुनिया जितनी आधुनिक, तेज़ और तकनीकी रूप से उन्नत होती जा रही है, उतना ही स्पष्ट होता जा रहा है कि समाज की मानसिकता अब भी पिछली सदियों की पितृसत्तात्मक सोच से पूर्णतः मुक्त नहीं हुई है। विशेष रूप से महिलाओं की डिजिटल गोपनीयता को लेकर सामाजिक दृष्टिकोण बहुत अधिक नियंत्रक, संदेहपूर्ण और रूढ़िवादी बना हुआ है। इंटरनेट, स्मार्टफोन और सोशल मीडिया तक महिलाओं की पहुँच तो बढ़ी है, पर उनके डिजिटल अधिकारों को समानता, सम्मान और स्वतन्त्रता के स्थान पर "निगरानी", "नियंत्रण" और "नैतिकता" के चश्मे से देखा जाता है।

व्यावहारिक स्तर पर देखा जाए तो जब किसी पुरुष को तकनीक का उपयोग करते हुए सक्रिय या स्वतंत्र देखा जाता है, तो इसे स्वाभाविक माना जाता है, जबकि उसी व्यवहार को यदि कोई महिला प्रदर्शित करे, तो उस पर नैतिक, सामाजिक और सांस्कृतिक सवाल खड़े कर दिए जाते हैं। यही दोहरा मानदंड डिजिटल स्पेस में महिलाओं की मौजूदगी को चुनौतीपूर्ण बना देता है।

जब साइबर अपराध महिलाओं के खिलाफ होता है, तो अधिकांश स्थितियों में समाज का ध्यान अपराधी, उसके उद्देश्य या अपराध की गंभीरता पर नहीं जाता, बल्कि पीड़िता के ऑनलाइन व्यवहार पर प्रश्नचिन्ह लगाए जाते हैं—जैसे:

- "उसे अपनी तस्वीरें डालने की क्या ज़रूरत थी?"
- "इतनी रात तक ऑनलाइन क्यों थी?"
- "पुरुषों से बात करने से परहेज़ नहीं कर सकती थी?"

ये सवाल केवल शब्द भर नहीं बल्कि समाज की गहरी जड़ें जमा चुकी **victim blaming** संस्कृति का संकेत हैं। इस मानसिकता में अपराध का केंद्र महिला बन जाती है और वास्तविक अपराधी सामाजिक दृष्टि से अदृश्य या गौण हो जाता है। परिणामस्वरूप, पीड़ित महिलाएँ शर्म, अपराधबोध, सामाजिक आलोचना और सम्मान खोने के डर से कानूनी कार्रवाई करने में हिचकती हैं, जिससे अपराधियों को छूट मिल जाती है और साइबर हिंसा का दायरा बढ़ता जाता है।

लैंगिक सामाजिक संरचना में नियंत्रण, सुरक्षा के नाम पर निगरानी और निर्णय लेने की शक्ति प्रायः पुरुषों या परिवार के अन्य प्रभुत्वशाली सदस्यों के पास होती है। इस संदर्भ में मोबाइल पासवर्ड मांगना, सोशल मीडिया अकाउंट चेक करना, लोकेशन ट्रैकिंग ऐप इंस्टॉल कराना, या ऑनलाइन बातचीत पर रोक लगाना अक्सर "केयर" और "संरक्षण" के नाम पर जायज़ ठहराया जाता है। जबकि वास्तविकता में यह व्यवहार महिलाओं की निजी स्वतंत्रता, डिजिटल अखंडता और **व्यक्तिगत एजेंसी** का उल्लंघन है।

महिलाओं की डिजिटल उपस्थिति को अक्सर "जोखिमपूर्ण" मानकर नियंत्रित करने के प्रयास किए जाते हैं, जबकि यही नियंत्रण मानसिकता असमानता को वैध बनाती है। इस प्रकार, डिजिटल सुरक्षा केवल साइबर अपराध या तकनीकी चुनौती नहीं है, बल्कि यह महिला अधिकारों, लैंगिक समानता और सामाजिक न्याय से जुड़ा प्रश्न भी है। जब तक समाज पीड़िता पर सवाल उठाने की बजाय अपराधी की जवाबदेही तय करने की आदत विकसित नहीं करेगा, और जब तक महिलाओं की डिजिटल स्वतंत्रता को एक **मानवाधिकार** के रूप में स्वीकार नहीं किया जाएगा, तब तक साइबर उत्पीड़न, ऑनलाइन दुर्व्यवहार और डिजिटल असमानता जैसी समस्याएँ निरंतर बनी रहेंगी।

➢ निष्कर्ष व सुझाव

डिजिटल युग ने महिलाओं के सामाजिक, आर्थिक और बौद्धिक जीवन में एक अभूतपूर्व परिवर्तन की शुरुआत की है। आज महिलाएँ पढ़ाई, पेशेवर विकास, सामाजिक सहभागिता, उद्यमिता, राजनीतिक भागीदारी और आत्म-प्रस्तुति जैसे विभिन्न क्षेत्रों में डिजिटल माध्यमों का सक्रिय और प्रभावशाली उपयोग कर रही हैं। इंटरनेट और तकनीक ने उन्हें न केवल नई संभावनाएँ प्रदान की हैं, बल्कि खुद को अभिव्यक्त करने और वैश्विक स्तर पर जुड़ने का मंच भी दिया है। लेकिन इस विकास के समानांतर, डिजिटल दुनिया में महिलाओं की सुरक्षा, गोपनीयता और व्यक्तिगत स्वायत्तता पर गंभीर प्रश्न भी उभरकर सामने आए हैं। तकनीक के विस्तार के साथ-साथ महिलाओं को लक्षित साइबर हिंसा के रूपों में निरंतर वृद्धि हो रही है—जैसे साइबर स्टॉकिंग, पहचान की चोरी, डीपफेक, अवैध निगरानी, मॉर्फ्ड इमेज, ऑनलाइन उत्पीड़न और टेक्नो-सक्षम लैंगिक हिंसा। यह स्पष्ट करता है कि डिजिटल अपराध केवल तकनीकी अनियमितताओं का परिणाम नहीं हैं, बल्कि गहरी सामाजिक संरचनाओं, लैंगिक शक्ति-संतुलन और पितृसत्तात्मक दृष्टिकोण से भी संचालित होते हैं।

डिजिटल अपराधों की जटिलता इस तथ्य में निहित है कि ये अपराध अदृश्य होते हैं, सीमाहीन होते हैं, और तकनीक की गति के साथ निरंतर विकसित होते रहते हैं। डेटा-आधारित शक्ति संरचना, एल्गोरिथ्मिक निगरानी और कृत्रिम बुद्धिमत्ता ने इस समस्या को नए आयाम दिए हैं, जहाँ अपराधी की पहचान, उद्देश्य और स्रोत तक पहुँचना कई बार कठिन हो जाता है। चुनौती केवल तकनीक या कानून के स्तर पर नहीं है, बल्कि यह सामाजिक चेतना, लैंगिक समानता, नीति-निर्माण और न्याय व्यवस्था की कमियों से भी गहराई से जुड़ी हुई है। जब तक समाज महिला की डिजिटल उपस्थिति को सम्मान, अधिकार और स्वायत्तता के साथ नहीं स्वीकार करेगा और victim-blaming की प्रवृत्ति समाप्त नहीं होगी, तब तक डिजिटल न्याय और सुरक्षित साइबर स्पेस एक आदर्श ही बना रहेगा।

अतः महिलाओं की डिजिटल गोपनीयता का यह संकट तकनीकी, सामाजिक, सांस्कृतिक और संस्थागत संरचनाओं के पारस्परिक प्रभावों का परिणाम है। इसे दूर करने के लिए कानून, तकनीक, शिक्षा, जागरूकता और सामाजिक व्यवहार—सभी स्तरों पर समन्वित प्रयास आवश्यक हैं, ताकि डिजिटल स्पेस वास्तव में समावेशी, सुरक्षित और समान हो सके।

सुझाव-

1. डिजिटल शिक्षा और साइबर साक्षरता कार्यक्रम: महिलाओं, किशोरियों, शिक्षकों, अभिभावकों और डिजिटल उपयोगकर्ताओं के लिए नियमित प्रशिक्षण कार्यक्रम आयोजित किए जाएँ, जिनमें डेटा सुरक्षा, पासवर्ड प्रबंधन, डिजिटल सहमति, साइबर अपराध रिपोर्टिंग और गोपनीयता सेटिंग्स की समझ शामिल हो। इससे डिजिटल सशक्तिकरण व्यवहारिक एवं जागरूक नागरिकता में परिवर्तित होगा।

2. मजबूत डेटा संरक्षण अवसंरचना: सरकारी और निजी डिजिटल प्लेटफार्मों पर महिलाओं से संबंधित संवेदनशील डेटा के संग्रह, उपयोग और भंडारण हेतु सख्त सुरक्षा प्रोटोकॉल अनिवार्य किए जाएँ। एंड-टू-एंड एन्क्रिप्शन, डेटा स्टोरेज निगरानी, तृतीय पक्ष डेटा साझाकरण नियंत्रण और दंडात्मक प्रावधानों को प्रभावी रूप से लागू किया जाए।

3. Gender-Sensitive Artificial Intelligence Regulation Policy: AI आधारित तकनीकों के उपयोग, प्रशिक्षण डेटा और आउटपुट पर लैंगिक दृष्टिकोण अनिवार्य बनाया जाए। इसके लिए:

- एल्गोरिथ्मिक निष्पक्षता (Algorithmic Fairness)
- AI Ethics Review Board
- Deepfake Regulation Framework

© Shiksha Samvad| Received: 03 December 2025 | Accepted: 10 December 2025 | Published: 15 December 2025

- Consent-based AI Use Model लागू किए जाएँ, ताकि तकनीक महिलाओं के खिलाफ हथियार न बने, बल्कि सशक्तिकरण का माध्यम बने।

4. फास्ट-ट्रैक डिजिटल क्राइम न्याय व्यवस्था: महिलाओं से जुड़े साइबर अपराधों के लिए समर्पित हेल्पलाइन, महिला साइबर सेल, प्रशिक्षित डिजिटल फॉरेंसिक विशेषज्ञ, फास्ट-ट्रैक अदालतें और केंद्रीकृत शिकायत पोर्टल स्थापित किए जाएँ। इससे न्याय प्रक्रिया गति, पारदर्शिता और सुलभता के साथ आगे बढ़ सकेगी।

5. शिक्षा व्यवस्था में डिजिटल नैतिकता का समावेश: स्कूलों, कॉलेजों और तकनीकी संस्थानों के पाठ्यक्रम में डिजिटल नागरिकता, ऑनलाइन सम्मान, साइबर सहमति, ई-नैतिकता और जिम्मेदार ऑनलाइन व्यवहार को शामिल किया जाए, ताकि भविष्य की डिजिटल संस्कृति अधिक संवेदनशील, न्यायपूर्ण और सुरक्षित बन सके।

संदर्भ सूची:

1. Castells, Manuel. *The Rise of Network Society*, Wiley-Blackwell, 2014, p. 42.
2. Foucault, Michel. *Discipline and Punish: The Birth of the Prison*, Vintage Books, 1995, p. 201.
3. Lyon, David. *Surveillance Society*, Polity Press, 2018, p. 118.
4. Sharma, R. *Cyber Feminism and Indian Women*, Sage Publications, 2022, p. 63.
5. NFHS-5 Report, Ministry of Health and Family Welfare, Government of India, 2021, p. 214.
6. UN Women Report, Digital Gender Gap, 2023, p. 39.
7. Pew Research Center. "Gender and Online Safety", 2022, p. 17.
8. NCRB Cyber Crime Data Report, 2023, p. 51.
9. **Turkle, Sherry.** (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other.* MIT Press, Cambridge.
10. **Wajcman, Judy.** (2004). *TechnoFeminism.* Polity Press, Cambridge.
11. **Zuboff, Shoshana.** (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Public Affairs, New York.
12. **Bauman, Zygmunt & Lyon, David.** (2013). *Liquid Surveillance: A Conversation.* Polity Press, Cambridge.
13. **Nussbaum, Martha C.** (2011). *Creating Capabilities: The Human Development Approach.* Harvard University Press, Cambridge.
14. **Lyon, David.** (2015). *Surveillance Studies: An Overview.* Polity Press, Cambridge.
15. Foucault, Michel. *The Birth of Biopolitics*, Routledge, 2008, p. 72.
16. Lyon, David. *The Culture of Surveillance*, Polity Press, 2019, p. 101.
17. Wajcman, Judy. *TechnoFeminism*, Polity Press, 2004, p. 54.
18. Sharma, R. *Cyber Feminism and Indian Women*, Sage Publications, 2022, p. 87.
19. McLuhan, Marshall. *Understanding Media: The Extensions of Man*, MIT Press, 2018, p. 29.

20. Beck, Ulrich. *Risk Society: Towards a New Modernity*, Sage Publications, 1992, p. 45.

21. Delhi Police Cyber Safety Report, 2023, pp. 41–43.

22. Maharashtra Cyber Cell Case File – Cyber Harassment Unit, 2024, p. 57.

23. Ministry of Women and Child Development (2013). *The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.* Government of India, New Delhi.

24. Government of India (2023). *Digital Personal Data Protection Act, 2023.* Ministry of Electronics and Information Technology (MeitY), New Delhi.

25. NITI Aayog (2024). *Women and Digital Safety in India: Legal Framework, Challenges and Policy Roadmap.* Government of India Report, New Delhi.

Cite this Article:

डॉ श्वेता द्विवेदी, "डिजिटल युग में महिला गोपनीयता का संकट: डेटा सुरक्षा, स्वतंत्रता और सामाजिक दृष्टिकोण" *Shiksha Samvad International Open Access Peer-Reviewed & Refereed Journal of Multidisciplinary Research, ISSN: 2584-0983 (Online), Volume 03, Issue 02, pp.47-56, December 2025. Journal URL: https://shikshasamvad.com/*

CERTIFICATE

of Publication

This Certificate is proudly presented to

डॉ श्वेता द्विवेदी

For publication of research paper title

डिजिटल युग में महिला गोपनीयता का संकट: डेटा सुरक्षा, स्वतंत्रता और सामाजिक दृष्टिकोण

Published in 'Shiksha Samvad' Peer-Reviewed and Refereed Research Journal and E-ISSN: 2584-0983(Online), Volume-03, Issue-02, Month December 2025, Impact Factor-RPRI-3.87.

Dr. Neeraj Yadav
Editor-In-Chief

Dr. Lohans Kumar Kalyani
Executive-chief- Editor

Note: This E-Certificate is valid with published paper and the paper must be available online at: https://shikshasamvad.com/

DOI:- https://doi.org/10.64880/shikshasamvad.v3i2.7