

साइबर अपराधों से महिलाओं की गरिमा पर संकट : विधिक प्रावधानों की प्रभावशीलता का विश्लेषण

Jyoti Chandel

Scholar, Department of Law, Samrat Vikramaditya Vishwavidyalaya, Ujjain

Dr. Aruna Sethi

Professor and Guide, Government Law College, Ujjain

सारांश

महिलाओं के विरुद्ध बढ़ते साइबर अपराध डिजिटल युग में एक गंभीर सामाजिक-आर्थिक और विधिक चिंता का विषय बन गए हैं। ये अपराध – जैसे ऑनलाइन उत्पीड़न, साइबर स्टॉकिंग, **रेवेज पोर्न** (बदले की भावना से अश्लील सामग्री साझा करना) और छवि से छेड़छाड़ – न केवल पीड़िताओं की निजता और आत्मसम्मान को ठेस पहुंचाते हैं, बल्कि मानसिक स्वास्थ्य, प्रतिष्ठा और सुरक्षा पर भी दीर्घकालिक प्रभाव छोड़ते हैं। इस शोध आलेख में महिलाओं की गरिमा पर साइबर अपराधों से उत्पन्न संकट की व्यापक पड़ताल की गई है, साथ ही भारत में उपलब्ध कानूनी ढांचे की प्रभावशीलता का विश्लेषण किया गया है। **सूचना प्रौद्योगिकी अधिनियम, 2000** तथा भारतीय दंड संहिता की विभिन्न धाराओं द्वारा साइबर अपराधों पर काबू पाने के प्रयास हो रहे हैं, परंतु कई मामलों में कानूनी प्रावधान अपर्याप्त साबित हो रहे हैं। प्रमुख विधिक प्रावधानों और न्यायिक निर्णयों (जैसे *ऋतु कोहली* मामले, 2001) के अध्ययन से पता चलता है कि कानून समय के साथ विकसित तो हुआ है, परंतु अभी भी अपराधियों को रोकने एवं पीड़ितों को न्याय दिलाने में अनेक चुनौतियाँ बरकरार हैं। अंततः, इस आलेख में मुख्य बाधाओं की पहचान कर सुझाव दिए गए हैं कि किस प्रकार विधि-प्रवर्तन, नीतियों और जागरूकता उपायों में सुधार करके साइबर स्पेस को महिलाओं के लिए अधिक सुरक्षित बनाया जा सकता है।

प्रस्तावना

डिजिटल तकनीक और इंटरनेट के प्रसार ने संचार के नए द्वार खोले हैं, लेकिन साथ ही एक नई चुनौतीपूर्ण दुनिया – **साइबर जगत** – में अपराधों को जन्म दिया है। विशेषकर महिलाएँ ऑनलाइन हिंसा और उत्पीड़न



का आसान शिकार बन रही हैं। सोशल मीडिया, ईमेल, चैट रूम जैसे मंचों पर अनचाहे संदेश, अश्लील सामग्री, धमकियाँ और मानहानि **महिलाओं की गरिमा** को चोट पहुँचा रही हैं। यह समस्या केवल तकनीकी नहीं, बल्कि सामाजिक-पितृसत्तात्मक सोच का डिजिटल विस्तार है, जहाँ वास्तविक जीवन में विद्यमान लैंगिक असमानता इंटरनेट पर भी दिखाई देती है (Agarwal, 2019)। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (NCRB) के आँकड़े दर्शाते हैं कि महिलाओं के विरुद्ध साइबर अपराध तेज़ी से बढ़ रहे हैं। *Crime in India 2021* रिपोर्ट के अनुसार वर्ष 2021 में ऐसे 17,950 मामले दर्ज हुए, जो पिछले वर्ष से 16.8% अधिक थे (राष्ट्रीय अपराध रिकॉर्ड ब्यूरो, 2022)। वर्ष 2022 में इनमें और 11% वृद्धि दर्ज की गई, जिसमें विशेषकर महिलाओं की आपत्तिजनक सामग्री ऑनलाइन प्रकाशित करने के मामलों में उछाल देखा गया – 2021 में 1,896 की तुलना में 2022 में 2,251 मामले दर्ज हुए (राजकुमार, 2023)। अन्य श्रेणियों (ब्लैकमेल, बदनाम करना, फ़र्ज़ी प्रोफ़ाइल से छेड़छाड़ आदि) में भी सैकड़ों मामले प्रति वर्ष दर्ज हो रहे हैं। यह तो केवल दर्ज मामलों की संख्या है; वास्तविक घटनाएँ इससे कहीं अधिक होने की संभावना है, क्योंकि बदनामी या अज्ञानता के भय से कई महिलाएँ शिकायत दर्ज ही नहीं करा पातीं (Agarwal, 2019)।

सर्वेक्षण भी इस समस्या की गंभीरता उजागर करते हैं। **राष्ट्रीय महिला आयोग (NCW)** के एक अध्ययन में पाया गया कि 54.8% महिलाओं ने किसी न किसी रूप में ऑनलाइन उत्पीड़न का अनुभव किया है, तथा करीब 26% महिलाओं की तस्वीरों या वीडियो के साथ छेड़छाड़ (morphing) की घटनाएँ सामने आई हैं (National Commission for Women, 2020)। ऐसे ऑनलाइन हमलों के परिणामस्वरूप पीड़िताओं में भय, तनाव, अवसाद आदि मनोवैज्ञानिक प्रभाव देखे गए हैं और कई बार उनकी सामाजिक प्रतिष्ठा व रोजगार पर नकारात्मक असर पड़ा है। वस्तुतः, इंटरनेट की अनामिता, व्यापक पहुँच और तीव्र गति – जो उसे अभिव्यक्ति का सशक्त माध्यम बनाती हैं – उसी का दुरुपयोग होने पर महिलाओं के खिलाफ शोषण के उपकरण बन जाते हैं। जो महिलाएँ राजनीति, मीडिया, सामाजिक कार्य जैसे सार्वजनिक जीवन में सक्रिय हैं, उन्हें विशेष रूप से संगठित ट्रोलिंग और ऑनलाइन बदनाम करने के हमलों का सामना करना पड़ता है, जिसके पीछे समाज की गहरी पितृसत्तात्मक धारणाएँ कार्यरत हैं (Ahlawat & Sharma, 2024)।

सरकार एवं विधि-प्रवर्तन एजेंसियों ने महिलाओं के लिए इंटरनेट को सुरक्षित बनाने के कई कदम उठाए हैं। भारत में वर्तमान **कानूनी ढाँचा** मुख्यतः *सूचना प्रौद्योगिकी अधिनियम, 2000* (IT Act) और भारतीय दंड संहिता (IPC) की धाराओं के मेल से निर्मित होता है, जो साइबर अपराधों से निपटने का आधार प्रदान करता है। हाल के वर्षों में *राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल* की शुरुआत, हेल्पलाइन 1930 की स्थापना, तथा



“Cyber Crime Prevention against Women and Children (CCPWC)” जैसे कार्यक्रमों द्वारा शिकायत दर्ज कराने और पुलिस प्रशिक्षण को सुगम बनाया गया है। विधिक स्तर पर भी सुधार जारी हैं – अगस्त 2023 में केंद्र सरकार ने भारतीय दंड संहिता के स्थान पर नया *भारतीय न्याय संहिता, 2023 (BNS)* विधेयक प्रस्तुत किया है, जिसमें साइबर स्टॉकिंग, डॉक्सिंग जैसी नई चुनौतियों के लिए प्रावधान शामिल करने का प्रस्ताव है (Ministry of Home Affairs, 2023)। इन पहलों के बावजूद ज़मीनी सच्चाई यह है कि पीड़ित महिलाओं को पर्याप्त न्याय मिलना अभी भी कठिन बना हुआ है। कई मामलों में या तो कानून में कमी है, या लागू प्रावधानों का प्रभावी क्रियान्वयन नहीं हो पाता। इसी परिप्रेक्ष्य में, **इस अध्ययन का उद्देश्य** महिलाओं के विरुद्ध साइबर अपराधों की प्रकृति तथा उनसे निपटने हेतु भारतीय विधिक प्रावधानों की प्रभावशीलता का समीक्षात्मक विश्लेषण करना है।

विधिक ढांचा: कानून और साइबर अपराध

भारतीय कानूनी प्रणाली ने साइबर अपराधों को नियंत्रित करने के लिए विभिन्न अधिनियमों और धाराओं का सहारा लिया है। सूचना प्रौद्योगिकी अधिनियम, 2000 (2008 में संशोधित) देश का प्रमुख साइबर कानून है, जिसमें हैकिंग, डाटा चोरी, पहचान की चोरी, obscenity (अश्लील सामग्री) के प्रसारण आदि कई अपराधों के लिए सज़ा का प्रावधान है। इसी प्रकार, भारतीय दंड संहिता (IPC) की पारंपरिक धाराओं को समय-समय पर संशोधित कर ऑनलाइन अपराधों पर लागू किया गया है – उदाहरणस्वरूप **क्रिमिनल लॉ (संशोधन) अधिनियम, 2013** द्वारा IPC में धारा 354D जोड़ी गई, जिसने पहली बार **साइबर स्टॉकिंग** को स्पष्ट रूप से अपराध की श्रेणी में परिभाषित किया (अपराधी के लगातार ऑनलाइन पीछा करने पर दंड)। इससे पूर्व, *ऋतु कोहली बनाम मनिष काठुरिया* (2001) देश का पहला साइबर स्टॉकिंग मामला था, जिसमें अभियुक्त ने एक महिला के नाम से अश्लील संदेश ऑनलाइन पोस्ट किए और उसका फोन नंबर सार्वजनिक कर उसे प्रताड़ित किया। उस समय विशिष्ट कानून के अभाव में अपराधी पर IPC की धारा 509 (महिला की लज्जा भंग करना) तथा आईटी एक्ट की सामान्य धाराओं के तहत मामला चलाया गया। यह घटना कानून में मौजूद खाई को उजागर करती है और इसी के परिणामस्वरूप बाद में *stalking* को परिभाषित करने वाला प्रावधान जोड़ा गया (World Pulse, 2015)।



नीचे तालिका में महिलाओं के विरुद्ध आम साइबर अपराधों और उनसे संबंधित मुख्य क़ानूनी प्रावधानों का सार दिया गया है:

महिलाओं के विरुद्ध साइबर अपराध	प्रमुख कानूनी प्रावधान (भारतीय कानून)
साइबर स्टॉकिंग / पीछा (बार-बार ऑनलाइन निगरानी या संपर्क करना)	IPC धारा 354D – पीछा करना (शारीरिक अथवा ऑनलाइन); IPC धारा 507 – अनाम रूप से डराना-धमकाना (यदि भय पैदा किया जाए)
ऑनलाइन यौन उत्पीड़न / ट्रोलिंग (गाली-गलौज, धमकी, अश्लील टिप्पणियाँ)	IPC धारा 354A – यौन उत्पीड़न (शारीरिक/ऑनलाइन); IPC धारा 509 – शब्दों/इशारों द्वारा स्त्री की लज्जा भंग करना
रेवेज पोर्न / गैर-सहमति अंतरंग सामग्री का प्रसार (बदले की भावना से निजी अश्लील चित्र/वीडियो साझा करना)	IT Act 2000 धारा 66E – निजता का उल्लंघन (निजी चित्र बिना सहमति प्रकाशित); IT Act 2000 धारा 67/67A – अश्लील एवं यौन रूप से स्पष्ट सामग्री का इलेक्ट्रॉनिक प्रसारण (पहली बार पर 3-5 वर्ष कारावास एवं जुर्माना); IPC धारा 354C – वीडियोग्राफी (किसी स्त्री की निजी गतिविधि की छुपकर तस्वीर लेना/बाँटना)
मॉर्फिंग एवं डीपफेक (तस्वीर/वीडियो से छेड़छाड़ कर अश्लील बनाना)	IT Act 2000 धारा 66C – पहचान की चोरी (किसी की डिजिटल पहचान का दुरुपयोग); IT Act 2000 धारा 67/67A – अश्लील/आपत्तिजनक सामग्री का प्रकाशन; IPC धारा 500 – मानहानि (यदि छवि/वीडियो से प्रतिष्ठा धूमिल की जाए)
साइबर मानहानि (ऑनलाइन बदनामी, झूठी अफ़वाह फैलाना)	IPC धारा 499/500 – मानहानि के लिए दंड (2 वर्ष तक कारावास या जुर्माना);



	IT Act 2000 धारा 67 – इलेक्ट्रॉनिक रूप में आपत्तिजनक/अपमानजनक सामग्री प्रकाशित करना
पहचान की चोरी / प्रतिरूपण (फ़र्जी प्रोफ़ाइल, पासवर्ड चुराना)	IT Act 2000 धारा 66C – किसी व्यक्ति की पहचान (आईडी/पासवर्ड) चुराना; IT Act 2000 धारा 66D – व्यक्ति बनकर धोखा देना (Online Impersonation)
डॉक्सिंग (किसी व्यक्ति की निजी जानकारी सार्वजनिक करना)	वर्तमान में कोई विशिष्ट धारा नहीं; संबंधित प्रावधान: IPC धारा 354D (पीछा करने में निजी जानकारी का दुरुपयोग) एवं IPC धारा 507 (अनाम धमकी) परिस्थितिनुसार लागू; BNS 2023 के मसौदे में पहली बार डॉक्सिंग को अपराध परिभाषित करने का प्रस्ताव (Ministry of Home Affairs, 2023)

उपर्युक्त कानूनी प्रावधान मिलकर एक व्यापक **विधिक ढाँचा** तैयार करते हैं जो साइबर अपराधों से निपटने का प्रयास करता है। उदाहरण के लिए, IPC की धाराएँ 354A, 354C, 354D विशेष रूप से यौन उत्पीड़न, Voyeurism और पीछा करने जैसे अपराधों को कवर करती हैं, वहीं आईटी एक्ट की धाराएँ 66E, 67, 67A अश्लील एवं निजी सामग्री के गैर-अधिकृत प्रसार को दंडित करती हैं। हालांकि, कई प्रावधानों के बावजूद, **कानून की प्रभावशीलता** सवाल के घेरे में है। कुछ अपराधों (जैसे डॉक्सिंग, गैर-सहमति से अंतरंग सामग्री प्रसार) के लिए अब तक स्पष्ट धाराएँ न होने के कारण अपराधियों पर मौजूदा कानून के तहत ही कार्यवाही चलानी पड़ती है, जो हमेशा पर्याप्त सिद्ध नहीं होती (Banerjee, 2019)। इसके अलावा, आईटी एक्ट की धारा 66A (अपमानजनक ऑनलाइन संदेश भेजने से संबंधित) को 2015 में *श्रेया सिंहल बनाम भारत संघ* मामले में असंवैधानिक करार देकर हटा दिया गया था, जिसके बाद से ऑनलाइन उत्पीड़न से निपटने के लिए कानून लागू करने वालों के पास एक उपकरण कम हो गया। इस संदर्भ में नए विधेयक (BNS, 2023) और मौजूदा कानूनों में संशोधन की पहल को सशक्त कानूनी ढाँचे की दिशा में सकारात्मक कदम कहा जा सकता है।



प्रमुख न्यायिक निर्णय

विभिन्न न्यायालयों ने समय-समय पर ऐसे मामलों में महत्वपूर्ण मिसालें पेश की हैं, जिन्होंने कानूनी ढाँचे की कमियों और संभावनाओं को उजागर किया। **ऋतु कोहली बनाम मनिष काठुरिया (2001)** केस, जैसा ऊपर उल्लेख हुआ, भारत का पहला दर्ज *साइबर स्टॉकिंग* का मामला था। इसमें अभियुक्त ने एक महिला की पहचान का दुरुपयोग कर अश्लील चैट संदेश पोस्ट किए और उनका फोन नंबर सार्वजनिक कर दिया, जिससे पीड़िता को भयंकर मानसिक प्रताड़ना झेलनी पड़ी। दिल्ली पुलिस ने सूचना प्रौद्योगिकी अधिनियम की मदद से तकनीकी साक्ष्य जुटाकर आरोपी को IPC धारा 509 के तहत गिरफ्तार किया। यद्यपि तब कोई विशिष्ट धारा उपलब्ध नहीं थी, यह निर्णय एक निर्णायक मोड़ साबित हुआ जिसने *साइबर पीछा* जैसे अपराधों को कानूनी मान्यता दिलाने की राह प्रशस्त की (World Pulse, 2015)। अंततः 2013 के संशोधन द्वारा IPC में धारा 354D सम्मिलित की गई, जिससे ऐसे मामलों में स्पष्ट कानूनी आधार मिला।

हाल के एक महत्वपूर्ण मामले **किर्ति वशिष्ठ बनाम राज्य (NCT दिल्ली), 2019** में दिल्ली उच्च न्यायालय ने एक आरोपी को एक महिला का निजी आपत्तिजनक वीडियो इंटरनेट पर अपलोड करने के अपराध में दोषी ठहराया। अदालत ने सूचना प्रौद्योगिकी अधिनियम की धारा 67 और 67A (अश्लील व यौन सामग्री का प्रसारण) तथा IPC की धाराओं का प्रयोग करते हुए आरोपी को सज़ा सुनाई (Delhi High Court, 2019)। यह *रेवेंज पोर्न* से संबंधित भारत के प्रारंभिक दृढ़ दोषसिद्धि मामलों में से एक था, जिसने संदेश दिया कि डिजिटल माध्यम पर किसी की अंतरंग सामग्री बिना सहमति प्रसारित करना एक गंभीर अपराध है। इसी तरह, केरल उच्च न्यायालय ने **Sri. Surya बनाम राज्य (केरल), 2022** मामले में लगातार ऑनलाइन उत्पीड़न (साइबर स्टॉकिंग) के आरोपी को IPC 354D और आईटी एक्ट की धाराओं के तहत दंडित किया (Kerala High Court, 2022)। इन न्यायिक निर्णयों से दो अहम निष्कर्ष निकलते हैं: प्रथम, मौजूदा कानूनों के दायरे में रहते हुए भी न्यायालय गंभीर साइबर अपराधों पर सख्त रुख अपनाने लगे हैं; द्वितीय, न्यायालयों ने सरकार का ध्यान उन कानूनी ख़ाओं की ओर आकर्षित किया है जहाँ नए प्रकार के ऑनलाइन अपराधों से निपटने हेतु विशिष्ट प्रावधानों की दरकार है (Drishti Judiciary, 2025)। उदाहरणस्वरूप, **X बनाम भारत संघ व अन्य** (मद्रास हाईकोर्ट, 2025) में अदालत ने डॉक्सिंग व साइबर उत्पीड़न की एक गंभीर घटना पर पुलिस और मध्यवर्ती (इंटरमीडियरी) की जिम्मेदारी तय करते हुए केंद्र को निर्देश दिए कि वह ऐसे मामलों के लिए ठोस कानून और त्वरित शिकायत निवारण तंत्र विकसित करे (Drishti Judiciary, 2025)। न्यायपालिका



के ये कदम पीड़ितों को आंशिक राहत देने के साथ-साथ विधि निर्माताओं को भी विधानों की खामियाँ दूर करने की ओर प्रेरित कर रहे हैं।

चुनौतियाँ

वर्तमान कानूनी प्रावधानों के बावजूद, महिलाओं के विरुद्ध साइबर अपराधों से प्रभावी रूप से निपटने में कई चुनौतियाँ सामने आती हैं (Muskan, 2025; Agarwal, 2019):

- **कानूनी खामियाँ और अपर्याप्त प्रावधान:** तकनीक के तेज विकास के चलते अपराध के नए रूप सामने आ रहे हैं, जबकि कानून अक्सर उनके पीछे चलते हैं। डॉक्सिंग, गैर-सहमति से अंतरंग सामग्री साझा करना (revenge porn) जैसे अपराधों पर सीधा रोक लगाने हेतु अब तक कोई विशिष्ट धारा नहीं बनी है (Banerjee, 2019)। मौजूदा प्रावधानों को उनके व्यापक अर्थ के तहत मजबूरन लागू करना पड़ता है, जिससे न्याय प्रक्रिया कमज़ोर हो सकती है।
- **अनुश्रवण और साक्ष्य जुटाने में दिक्कत: अनामिता (anonymity)** और इंटरनेट की सीमा-रहित प्रकृति के कारण अपराधियों को पहचान पाना कठिन हो जाता है। साइबर अपराधी प्रायः फ़र्ज़ी प्रोफ़ाइल, वीपीएन, और गुप्त ऐप्स का प्रयोग कर अपना पता छिपाते हैं। डिजिटल साक्ष्यों को सुरक्षित एकत्र करना व प्रमाणित करना तकनीकी रूप से जटिल और महंगा है। कई बार अंतरराष्ट्रीय सर्वरों या क्लाउड स्टोरेज से डाटा प्राप्त करना लंबी न्यायिक सहायताओं पर निर्भर करता है, जिस कारण जांच में देरी होती है।
- **अपराध रिपोर्ट करने में झिझक (Underreporting):** सामाजिक कलंक, बदनामी का डर और कानून प्रवर्तन पर अविश्वास जैसे कारणों से महिलाओं द्वारा साइबर अपराध की शिकायत ही दर्ज नहीं की जाती। पीड़िताएँ आशंकित रहती हैं कि पुलिस या समाज उनके आरोपों को गंभीरता से नहीं लेगा, उल्टे उन्हें ही दोष दिया जा सकता है (victim blaming)। नतीजतन, वास्तविक घटनाओं और दर्ज मामलों के बीच बड़ा अंतर रहता है (Agarwal, 2019)।
- **प्रवर्तन एवं संसाधन की कमी:** स्थानीय पुलिस थानों में अक्सर साइबर फ़ॉरेंसिक विशेषज्ञता या प्रशिक्षित कर्मियों का अभाव होता है। सीमित संसाधन, तकनीकी औज़ारों की कमी तथा भारी कार्यभार के चलते कई मामले ठीक से जांच से पहले ही ठंडे पड़ जाते हैं। विशेषकर छोटे शहरों में साइबर सेल का अभाव या अपर्याप्तता भी एक बड़ी बाधा है।



- **धीमी न्याय प्रक्रिया:** भारत में न्यायालयों में मामलों का बड़ा लंबित भार है। साइबर अपराध के मामलों में सबूतों की तकनीकी प्रकृति के कारण मुकदमों के निपटारे में अतिरिक्त समय लगता है। लंबी खिंचती कानूनी लड़ाईयों से कई पीड़ित हताश होकर बीच में ही मुकदमा छोड़ देते हैं या समझौता करने को मजबूर हो जाते हैं (Kumar & Yadav, 2021)।
- **सोशल मीडिया प्लेटफॉर्म और मध्यवर्तियों की भूमिका:** आपत्तिजनक सामग्री को हटाने और अपराधियों की जानकारी देने में कई बार प्लेटफॉर्म देरी करते हैं या सहयोग नहीं करते। हालांकि आईटी (मध्यवर्ती दिशानिर्देश) नियम, 2021 के तहत शिकायत मिलने पर 24 घंटे में आपत्तिजनक सामग्री हटाने का प्रावधान है, इसका सख्त पालन सुनिश्चित करना चुनौती बना हुआ है।

इन चुनौतियों के चलते **कानूनी प्रभावशीलता** प्रभावित होती है। कानून भले ही मौजूद हों, किन्तु जब तक उनका क्रियान्वयन तेज़, सुलभ और पीड़िता के अनुकूल न हो, तब तक साइबर स्पेस में महिलाओं की सुरक्षा अधूरी रहेगी। मौजूदा परिदृश्य में तकनीक और कानून के बीच की दूरी को पाटने की आवश्यकता है, ताकि **न्याय की पहुंच** डिजिटल युग में भी उतनी ही प्रभावी हो जितनी वास्तविक जगत में।

निष्कर्ष एवं सुझाव

अभ्यासतः, महिलाओं के खिलाफ साइबर अपराध आधुनिक समाज में **लैंगिक हिंसा** का नया आयाम हैं, जो उनकी गरिमा, स्वतंत्रता और डिजिटल भागीदारी पर सीधा प्रहार करते हैं। उपर्युक्त अध्ययन से स्पष्ट है कि भारत ने कानूनी ढांचे के जरिए इन अपराधों से निपटने की बुनियाद रखी है, परंतु बदलते तकनीकी परिदृश्य के साथ कानून के अद्यतन और दृढ़ अनुपालन की तत्काल आवश्यकता है। **कानूनी प्रावधानों की प्रभावशीलता** का आकलन करते हुए पाया गया है कि जहाँ कुछ धाराओं ने अपराधियों को सज़ा दिलाने में सफलता पाई (जैसे IPC 354D, IT Act 67A के तहत हालिया सजाएँ), वहीं कई अपराध अब भी स्पष्ट परिभाषा या दंड के दायरे से बाहर हैं, जिससे पीड़िताओं को पूर्ण न्याय नहीं मिल पा रहा। इस चुनौतीपूर्ण समस्या से निपटने के लिए बहुआयामी प्रयास आवश्यक हैं। निम्नलिखित **सुझाव** इस दिशा में सहायक हो सकते हैं:

- **कानूनी सुधार व नया कानून:** *भारतीय न्याय संहिता (BNS), 2023* जैसे नए विधेयक को शीघ्र लागू करके साइबर स्टॉकिंग, डॉक्सिंग, गैर-सहमति पोर्नोग्राफी जैसे अपराधों के लिए स्पष्ट धाराएँ बनाई जाएँ। साथ ही आईटी अधिनियम में महिलाओं की ऑनलाइन सुरक्षा हेतु विशेष उपबंध जोड़े जाएँ।



कानूनों की भाषा को तकनीकी परिवर्तनों के अनुसार निरंतर अद्यतन करना होगा (Ministry of Home Affairs, 2023)।

- **तेज़ और विशेषीकृत न्याय प्रक्रिया:** साइबर अपराध मामलों के शीघ्र निपटान हेतु विशेष फास्ट-ट्रैक न्यायालयों की स्थापना हो। न्यायाधीशों और अभियोजकों को साइबर कानून व डिजिटल साक्ष्यों का प्रशिक्षण दिया जाए। डिजिटल सबूतों की जांच के लिए आधुनिक फॉरेंसिक प्रयोगशालाएँ स्थापित कर उन्हें न्यायिक मान्यता दी जाए, ताकि प्रमाणिकता पर सवाल न उठें।
- **पुलिस बल का सशक्तिकरण:** प्रत्येक ज़िले में समर्पित **साइबर सेल** या **महिला साइबर अपराध इकाई** का गठन हो, जहाँ प्रशिक्षित महिला एवं पुरुष कर्मी हों। पुलिस को नवीनतम साइबर सुरक्षा तकनीकों, ट्रैकिंग टूल्स और गोपनीयता कानूनों का प्रशिक्षण दिया जाए (Muskan, 2025)। केंद्रीय व राज्य स्तर पर *IAC (Indian Cyber Crime Coordination Centre)* जैसी पहल को मज़बूती से लागू किया जाए।
- **सामाजिक जागरूकता और डिजिटल साक्षरता:** महिलाओं एवं आमजन में जागरूकता बढ़ाना उतना ही ज़रूरी है जितना कानून बनाना। स्कूलों, कॉलेजों में **साइबर सुरक्षा एवं डिजिटल शिष्टाचार** के कार्यक्रम चलाए जाएँ (Mehta, 2020)। महिलाएँ स्वयं किस प्रकार ऑनलाइन खतरों से बचाव कर सकती हैं (जैसे गोपनीयता सेटिंग्स, सुरक्षित पासवर्ड, संदिग्ध संदेशों को अनदेखा करना) – इस बारे में अभियान चलाए जाएँ। परिवार और समाज में भी यह संदेश जाए कि पीड़िता को दोष देने के बजाय अपराधी को दंडित करना महत्वपूर्ण है।
- **शिकायत तंत्र को सुदृढ़ बनाना:** राष्ट्रीय साइबर पोर्टल और 112/1930 हेल्पलाइन को और प्रभावी बनाया जाए। शिकायत दर्ज करने की प्रक्रिया सरल, गोपनीय और पीड़िता के अनुकूल हो ताकि अधिक महिलाएँ आगे आएँ। दर्ज शिकायतों पर पुलिस की जवाबदेही तय हो – जैसे निश्चित समय-सीमा में प्राथमिक जाँच पूरी करना और पीड़िता को प्रगति से अवगत कराना।
- **मध्यवर्तियों की जवाबदेही:** सोशल मीडिया प्लेटफ़ॉर्म, वेबसाइट एवं इंटरनेट सेवा प्रदाताओं को कड़ी निगरानी में रखते हुए यह सुनिश्चित किया जाए कि वे शिकायत मिलते ही घृणित/अश्लील सामग्री तुरंत हटाएँ (नियमों द्वारा निर्धारित 24 घंटे की समयसीमा में)। नियामक निकाय इन प्लेटफ़ॉर्म की नियमित ऑडिट करें और गैर-अनुपालन पर आर्थिक दंड या लाइसेंस निलंबन जैसे कड़े कदम उठाए जाएँ (Bhat, 2021)।



- **अंतर्राष्ट्रीय सहयोग:** चूँकि साइबर अपराध प्रायः सीमाओं के पार होते हैं, कानून प्रवर्तन एजेंसियों को अंतर्राष्ट्रीय स्तर पर समन्वय बढ़ाना होगा। डेटा साझाकरण, प्रत्यार्पण संधि और *बुडापेस्ट कन्वेंशन* जैसे समझौतों के माध्यम से अपराधियों को विदेश में भी न्याय के कटघरे में लाना संभव हो सकेगा।

अंत में, तकनीक के युग में महिलाओं की गरिमा और अधिकारों की रक्षा के लिए एक समेकित दृष्टिकोण की आवश्यकता है, जिसमें मजबूत कानून, तत्पर प्रवर्तन, जागरूक समाज और उत्तरदायी तकनीकी मंच – सभी की भूमिका अहम है। यदि उपर्युक्त सुझावों पर अमल किया जाए तो इंटरनेट को महिलाओं के लिए भयमुक्त और समानता-पूर्ण बनाने की दिशा में महत्वपूर्ण प्रगति हासिल की जा सकती है। एक सुरक्षित साइबर स्पेस न केवल महिलाओं के **मानवाधिकारों** को सुनिश्चित करेगा, बल्कि डिजिटल इंडिया के लक्ष्य को वास्तविक अर्थों में सबके लिए सशक्त बनाएगा।

संदर्भ सूची

- [1]. Agarwal, S. (2019). *Cyber Crimes Against Women in India: Legal Framework and Challenges*. **Journal of Law and Social Policy**, 12(1), 45–67.
- [2]. Ahlawat, H., & Sharma, S. (2024). *Cyber Crimes Against Women in India*. **ShodhKosh: Journal of Visual and Performing Arts**, 5(6), 1539–1544. DOI: 10.29121/shodhkosh.v5.i6.2024.2430
- [3]. Banerjee, P. (2019). *Revenge Porn and the Law: A Global and Indian Perspective*. **International Journal of Law & IT**, 5(3).
- [4]. Delhi High Court (2019). *Kirti Vashisht v. State of NCT of Delhi*, 2019 SCC OnLine Del 11713. (दिल्ली उच्च न्यायालय का रेवेज पोर्न संबंधी निर्णय)
- [5]. Drishti Judiciary (2025). "Cyber Harassment on Women." *To The Point* (Online series). (Madras HC, 2025 केस व विधिक प्रावधानों पर टिप्पणी)
- [6]. Ministry of Home Affairs (2023). *Bharatiya Nyaya Sanhita, 2023* (Bill No. __ of 2023). (उपनिवेशकालीन IPC के स्थान पर प्रस्तावित नया दंड संहिता विधेयक)
- [7]. National Commission for Women (2020). *Research Study on Cyber Harassment*. (54.8% महिलाओं के ऑनलाइन उत्पीड़न से संबंधित NCW सर्वेक्षण रिपोर्ट)



- [8]. National Crime Records Bureau (2022). *Crime in India 2021 – Statistics*. Ministry of Home Affairs, Government of India. (साइबर अपराध से संबंधित आधिकारिक वार्षिक आंकड़े)
- [9]. Rajkumar, A. (2023, December 5). "Crimes against women rise by 4%, cyber crimes increase by 11%: NCRB data." *The News Minute*.
- [10]. World Pulse (2015). "Cyber Stalking – A 'Virtual' Crime With Real Consequences." (Mukut द्वारा ऋतु कोहली प्रकरण पर लेख)
- [11]. Muskan. (2025). "Cybercrime Against Women in India: A Comprehensive Study." *International Research Journal of Modernization in Engineering, Technology and Science*, 7(4).

