National Journal of Multidisciplinary Research and Development
www.newresearchjournal.com
ISSN: 2455-9040
Received: 30-11-2025, Accepted: 30-12-2025, Published: 14-01-2026
Volume 11, Issue 1, 2026, Page No. 26-32

तकनीकी के दौर में महिलाओं, बच्चों और कमजोर वर्गों के विरुद्ध बढ़ते अपराध: एक विश्लेषणात्मक अध्ययन

अतुल कुमार यादव
शोध छात्र, विधि संकाय, सोबन सिंह जीना विश्वविद्यालय, अल्मोड़ा, उत्तराखंड, भारत

सारांश
सूचना एवं संचार प्रौद्योगिकी के तीव्र विकास ने समकालीन समाज की संरचना, व्यवहार और संबंधों को गहराई से प्रभावित किया है। इंटरनेट और डिजिटल प्लेटफॉर्मों के माध्यम से जहाँ ज्ञान, अभिव्यक्ति और सहभागिता का दायरा व्यापक हुआ है, वहीं इसी तकनीकी विस्तार ने अपराध के ऐसे नए आयाम भी उत्पन्न किए हैं, जो अदृश्य, सीमाहीन और त्वरित प्रकृति के हैं। डिजिटल स्पेस अब केवल सुविधा और सशक्तिकरण का माध्यम नहीं रहा, बल्कि महिलाओं, बच्चों और कमजोर वर्गों के लिए एक गंभीर सामाजिक–कानूनी चुनौती के रूप में उभर कर सामने आया है। यह शोध तकनीकी युग में भारत में महिलाओं, बच्चों, वरिष्ठ नागरिकों तथा सामाजिक रूप से वंचित वर्गों के विरुद्ध बढ़ते अपराधों का विश्लेषणात्मक अध्ययन प्रस्तुत करता है। साइबर–स्टॉकिंग, ऑनलाइन उत्पीड़न, डिजिटल मानहानि, मॉर्फिंग, पहचान–चोरी, अश्लील सामग्री का गैर–सहमति प्रसार, सेक्सटॉर्शन तथा साइबर पोर्नोग्राफी जैसे अपराध न केवल पीड़ित की निजता और गरिमा का उल्लंघन करते हैं, बल्कि उनके मानसिक स्वास्थ्य, सामाजिक प्रतिष्ठा और आर्थिक सुरक्षा को भी गम्भीर रूप से प्रभावित करते हैं। अध्ययन में यह रेखांकित किया गया है कि उपलब्ध आंकड़े साइबर अपराधों की वास्तविक स्थिति का पूर्ण प्रतिबिंब नहीं हैं, क्योंकि सामाजिक बदनामी, भय और विधिक प्रक्रिया की जटिलताओं के कारण बड़ी संख्या में अपराध रिपोर्ट ही नहीं हो पाते। हालाँकि भारतीय न्याय प्रणाली में औपनिवेशिक कानूनों के स्थान पर नई संहिताओं को लागू किया गया है, फिर भी साइबर–स्टॉकिंग, ऑनलाइन वित्तीय धोखाधड़ी और डिजिटल यौन अपराधों जैसे उभरते अपराधों के लिए विशिष्ट और व्यापक प्रावधानों का अभाव बना हुआ है।

मूल शब्दः साइबर अपराध, डिजिटल युग, महिलाएँ और बच्चे, कमजोर वर्ग, साइबर सुरक्षा, विधिक प्रावधान, डिजिटल साक्षरता

प्रस्तावना
आज का वैश्विक परिदृश्य वास्तव में क्या उस बिंदु पर पहुँच चुका है जहाँ कुछ भी पूर्णतः गोपनीय नहीं रह गया है? गहराई से विचार करने पर यह स्पष्ट होता है कि वर्तमान में काफी हद तक ऐसी परिस्थितियाँ उत्पन्न हो चुकी है, जिनमें रहस्य और निजता की अवधारणा निरंतर सिमटती जा रही है। तकनीकी प्रगति के इस युग में इंटरनेट ने भौगोलिक सीमाओं को अप्रासंगिक बनाते हुए सूचना, ज्ञान और संचार को आम जन तक सहज रूप से पहुँचाया है। वर्तमान समय में इंटरनेट न केवल समय की बचत का प्रभावी साधन बन गया है, बल्कि विभिन्न कार्यों पर होने वाले आर्थिक व्यय को भी उल्लेखनीय रूप से घटा चुका है। इसने जीवन को अधिक व्यवस्थित, सुगम और निश्चित बनाने में महत्वपूर्ण भूमिका निभाई है, किंतु इन सकारात्मक पहलुओं के समानांतर, साइबर जगत में अपराधों का एक विस्तृत और संगठित तंत्र भी विकसित हुआ है। पिछले कुछ वर्षों के दौरान भारत में महिलाओं, बच्चों तथा अन्य कमजोर वर्गों के विरुद्ध तकनीक–संचालित अपराधों में चिंताजनक वृद्धि देखने को मिली है। जो अपराध पहले केवल भौतिक समाज तक सीमित माने जाते थे, वे अब डिजिटल माध्यमों में नए रूपों के साथ सामने आ रहे हैं। इनमें ऑनलाइन छेड़छाड़, दुर्व्यवहार, उत्पीड़न और ब्लैकमेलिंग जैसी गतिविधियाँ प्रमुख हैं। तकनीकी विस्तार के साथ–साथ ईमेल के माध्यम से प्रताड़ना, साइबर स्टॉकिंग, मानहानि, डिजिटल छवि–विकृति (मॉर्फिंग), स्पूफिंग, हैकिंग, अश्लील सामग्री का प्रसार, सेक्स ट्रैफिकिंग और ऑनलाइन छेड़छाड़ जैसे अपराध महिलाओं, बच्चों और कमजोर वर्गों के लिए गंभीर चुनौती बनते जा रहे हैं। यह निर्विवाद है कि ज्ञान और अभिव्यक्ति की स्वतंत्रता के विस्तार ने सुविधाओं को बढ़ाया है, किंतु विकृत और आपराधिक मानसिकताओं द्वारा इस तकनीकी व्यवस्था के दुरुपयोग के मामले भी लगातार सामने आ रहे हैं। अगर आकड़ों की बात की जाए तो भारत में साइबर क्राइम रिपोर्ट 2022 के अनुसार–, साइबर अपराध के तहत कुल 65,893 मामले तथा वर्ष 2021 में 52,974 मामले दर्ज किए गए। जो तुलना में 24.4% की वृद्धि दर्शाता है। अपराध दर 2021 में 3.9 से बढ़कर 2022 में 4.8 हो गया। 2022 के दौरान, दर्ज किए गए साइबर अपराध के मामलों में से 64.8% धोखाधड़ी के उद्देश्य से थे (65,893 मामलों में से 42,710), इसके बाद जबरन वसूली 5. 5% (3,648 मामले) और यौन शोषण 5.2% (3,434 मामले) थे। महिलाओं के खिलाफ अपराधों से आगे बढ़कर बच्चों, वरिष्ठ नागरिकों, अनुसूचित जातियों और अनुसूचित जन जातियों के खिलाफ अपराधों में क्रमशः 8.7%, 9.3%, 13.1% और 14.3% की वृद्धि दर्शाते हैं। इसके अतिरिक्त, आर्थिक अपराधों में 11.1% की वृद्धि देखी गई, भ्रष्टाचार में 10.5% की वृद्धि हुई। दरअसल हम जिन आंकड़ों की बात कर रहे हैं वे सब रिपोर्टेड आंकड़े हैं। लेकिन ऐसे भी हजारों मामले में हैं जहां आरोपियों या समाज में बदनामी के डर से महिलाओं, बच्चों और कमजोर वर्गों के खिलाफ हो रहे अपराधों को रिपोर्ट नहीं किया जाता है। खराब आंकड़ों के लिए कुछ हद तक दोष इस तथ्य में भी है कि हमारे पास पर्याप्त कानून नहीं हैं। फिर भी तकनीकी आधारित अपराधों से अधिक प्रभावी ढंग से निपटने के लिए भारत में मौजूदा कानूनों को मजबूत करने और सख्ती से लागू करने की तत्काल आवश्यकता है। हालांकि औपनिवेशिक युग के कानूनों से भारतीय न्याय संहिता और भारतीय नागरिक सुरक्षा संहिता में बदलाव किया गया है। फिर भी नई संहिता में साइबरस्टॉकिंग और ऑनलाइन वित्तीय धोखाधड़ी जैसे डिजिटल युग के अपराधों से निपटने के लिए व्यापक प्रावधानों का अभाव है, जिनकी आज के तकनीकी रूप से संचालित समाज में प्रासंगिकता तीव्रता से बढ़ रही है।

तकनीकी आधारित अपराध का उद्भव
1980 के दशक के उत्तरार्ध में ई–मेल के व्यापक उपयोग के साथ तकनीक–आधारित अपराधों की पहली उल्लेखनीय लहर सामने आई। इस माध्यम ने इनबॉक्स के जरिए विभिन्न प्रकार के

वायरस और मैलवेयर के प्रसार को संभव बना दिया। इसके पश्चात 1990 के दशक में वेब ब्राउज़रों के आगमन ने इंटरनेट उपयोग को सरल बनाया, किंतु इसी दौरान संदिग्ध वेबसाइटों पर ब्राउज़िंग के समय साइबर अपराधियों द्वारा नेटवर्क कनेक्शन के माध्यम से वायरस को उपयोगकर्ताओं के कंप्यूटर सिस्टम तक पहुँचाया जाने लगा, जिससे उपकरणों की कार्यक्षमता प्रभावित होती थी। कुछ मैलवेयर अनचाहे पॉप–अप विज्ञापन प्रदर्शित करते थे, जबकि कुछ उपयोगकर्ताओं को अश्लील वेबसाइटों की ओर स्वतः रीडायरेक्ट कर देते थे। वास्तविक अर्थों में साइबर अपराधों का विस्तार 2000 के दशक के प्रारंभ में तब हुआ, जब "सोशल मीडिया" प्लेटफॉर्म अस्तित्व में आए। उपयोगकर्ताओं द्वारा प्रोफ़ाइल डेटाबेस में अत्यधिक व्यक्तिगत विवरण साझा किए जाने से अज्ञात अपराधियों को पहचान–चोरी, गोपनीयता का उल्लंघन, बैंक खातों तक अनधिकृत पहुँच, क्रेडिट कार्ड के दुरुपयोग तथा अन्य प्रकार की वित्तीय धोखाधड़ी करने के अवसर मिले। यद्यपि इंटरनेट आज के दैनिक जीवन का अभिन्न अंग बन चुका है, फिर भी महिलाओं, बच्चों और अन्य कमजोर वर्गों की सुरक्षा एक गंभीर और संवेदनशील चुनौती के रूप में उभरकर सामने आई है। सरकार द्वारा निगरानी गोपनीयता के उल्लंघन का सबसे नवीनतम स्वरूप है। सूचना प्रौद्योगिकी और सोशल मीडिया के तीव्र विकास के कारण व्यक्तिगत डेटा की सुरक्षा सुनिश्चित करना लगातार कठिन होता जा रहा है। आईसीटी, इंटरनेट और सोशल मीडिया के अत्यधिक उपयोग, सुरक्षा उपायों के प्रति लापरवाही तथा साइबर सुरक्षा संबंधी जागरूकता के अभाव के चलते तकनीक–आधारित अपराधों में निरंतर वृद्धि हो रही है। अनेक मोबाइल एप्लिकेशन और वेबसाइटें उपयोगकर्ताओं, विशेषकर महिलाओं से, गोपनीय जानकारियाँ प्राप्त करने के लिए आकर्षक माध्यमों का सहारा लेती हैं, जिसके परिणामस्वरूप उत्पीड़न, प्रतिरूपण, हैकिंग जैसे गंभीर साइबर अपराधों की घटनाएँ जन्म लेती हैं।

भारत में महिलाओं बच्चों व कमजोर वर्गों के विरुद्ध तकनीकी आधारित अपराध

भारतीय सभ्यता में प्राचीन काल से ही महिलाओं को देवीस्वरूप मानते हुए उन्हें सम्मान और पूजनीय स्थान प्रदान किया गया है। इसके बावजूद सामाजिक संरचना में उनकी विशेष स्थिति होने के बाद भी महिलाएँ व्यवहारतः समाज के सर्वाधिक संवेदनशील और कमजोर वर्गों में गिनी जाती रही हैं। ऐतिहासिक दृष्टि से देखा जाए तो बाहरी आक्रमणों के काल से भारत में महिलाओं के विरुद्ध अपराधों में निरंतर वृद्धि देखने को मिलती है। चाहे प्राचीन युग हो अथवा आधुनिक समय, महिलाओं के प्रति हिंसा और उत्पीड़न विभिन्न रूपों में विद्यमान रहे हैं। वर्तमान परिप्रेक्ष्य में अपराधों की प्रकृति और उनके निष्पादन का माध्यम परिवर्तित हो गया है। जो कृत्य पहले भौतिक समाज तक सीमित थे, वे अब डिजिटल मंचों पर स्थानांतरित हो चुके हैं। इस श्रेणी में ऑनलाइन छेड़छाड़, धमकियाँ देना, अपशब्दों का प्रयोग, शीलभंग, मानसिक उत्पीड़न तथा ब्लैकमेलिंग जैसे कृत्य शामिल हैं। सूचना प्रौद्योगिकी के आधुनिक युग में भारत में तकनीक–आधारित अपराधों का प्रभाव विशेष रूप से महिलाओं, बच्चों और अन्य कमजोर वर्गों पर पड़ रहा है। इन अपराधों में ईमेल के माध्यम से प्रताड़ना, साइबर स्टॉकिंग, साइबर मानहानि, डिजिटल छवि–विकृति (मॉर्फिंग), ईमेल स्पूफिंग, हैकिंग, साइबर पोर्नोग्राफी, साइबर सेक्स ट्रैफिकिंग, ऑनलाइन यौन मानहानि तथा डिजिटल छेड़छाड़ जैसी अनेक गतिविधियाँ सम्मिलित हैं, जो न केवल पीड़ितों की गरिमा और निजता को आघात पहुँचाती हैं, बल्कि सामाजिक सुरक्षा व्यवस्था के समक्ष भी गंभीर चुनौती प्रस्तुत करती हैं। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी) द्वारा प्रकाशित वार्षिक 'भारत में अपराध रिपोर्ट 2022' के अनुसार, महिलाओं, अनुसूचित जाति (एससी), अनुसूचित जनजाति (एसटी), बच्चों, साइबर अपराधों और राज्य के खिलाफ अपराधों में 2021 की तुलना में 2022 में वृद्धि देखी गई। 2022 के दौरान बच्चों के खिलाफ अपराध के कुल 1,62,449 मामले दर्ज किए गए, जो 2021 (1,49,404 मामले) की तुलना में 8.7% अधिक है। प्रतिशत के लिहाज से, 2021 के दौरान 'बच्चों के खिलाफ अपराध' के तहत अपराध के प्रमुख शीर्षक अपहरण और अपहरण (45.7%), और यौन अपराधों से बच्चों का संरक्षण (POCSO) अधिनियम, 2012 (39.7%) थे, जिसमें बाल बलात्कार भी शामिल है। 2022 के दौरान किशोरों के खिलाफ कुल 30,555 मामले दर्ज किए गए हैं, जो 2021 (31,170 मामले) की तुलना में 2% की गिरावट दर्शाता है। अपराध दर 2021 में 7% से घटकर 2022 में 6.9% हो जाने का अनुमान है। वरिष्ठ नागरिकों (60 वर्ष से अधिक) के खिलाफ अपराध करने के कुल 28,545 मामले दर्ज किए गए, जो 2021 (26,110 मामले) की तुलना में 9.3% की वृद्धि दर्शाता है। अनुसूचित जातियों के विरुद्ध अपराध के कुल 57,582 मामले दर्ज किए गए, जो 2021 (50,900 मामले) की तुलना में 13.1% की वृद्धि दर्शाते हैं। अनुसूचित जनजातियों (एसटी) के खिलाफ अपराध के कुल 10,064 मामले दर्ज किए गए, जो 2021 (8,802 मामले) की तुलना में 14.3% की वृद्धि दर्शाता है। साइबर अपराधों के तहत कुल 65,893 मामले दर्ज किए गए, जो 2021 (52,974 मामले) की तुलना में पंजीकरण में 24.4% की वृद्धि दर्शाता है। 2022 के दौरान, दर्ज किए गए साइबर अपराध के 64.8% मामले धोखाधड़ी (65,893 मामलों में से 42,710) के उद्देश्य से थे, इसके बाद 5.5% (3,648 मामले) जबरन वसूली और 5.2% (3,434 मामले) यौन शोषण के मामले थे।

बढ़ते हुए तकनीकी के दौर में डिजिटल अपराधों के प्रकार

1. **हैकिंग: य**ह एक विशिष्ट स्वरूप का अपराध है जो डिजिटल माध्यम से किया जाता है। जिसमें अपराधी अनधिकृत तरीके से कंप्यूटर प्रणालियों या नेटवर्क में प्रवेश करने का प्रयास करते हैं, ताकि उपलब्ध डेटा को चोरी किया जा सके, उसमें हेरफेर किया जाए अथवा उसे पूर्णतः नष्ट किया जा सके।

2. **मैलवेयर:** यह एक प्रकार का हानिकारक सॉफ़्टवेयर होता है, जिसे कंप्यूटर प्रणालियों के सामान्य संचालन में बाधा उत्पन्न करने, उन्हें क्षति पहुँचाने अथवा बिना अनुमति के सिस्टम तक पहुँच बनाने के उद्देश्य से तैयार किया जाता है। इसका मुख्य उद्देश्य पीड़ित की फ़ाइलों या डिजिटल डेटा को एन्क्रिप्ट कर उन्हें निष्क्रिय अवस्था में बंद कर देना होता है, जिसके पश्चात उन्हें पुनः उपलब्ध कराने के बदले पीड़ित से फिरौती की माँग की जाती है। इस तरह के साइबर अपराध सामान्यतः उन उपयोगकर्ताओं को अधिक प्रभावित करते हैं जिनका तकनीकी ज्ञान सीमित होता है। इस श्रेणी में वायरस, वर्म, ट्रोजन हॉर्स, रैंसमवेयर तथा स्पाइवेयर जैसे विभिन्न प्रकार के दुर्भावनापूर्ण प्रोग्राम सम्मिलित होते हैं।

3. **आनलाइन ग्रूमिंग:** आनलाइन ग्रूमिंग में आवश्यक रूप से दो या दो से अधिक व्यक्ति शामिल हो सकते है जो डिजिटल रूप संचार तकनीक द्वारा एक दूसरे से जुड़ें होते है और एक दूसरे से अनजान होते है। आनलाइन ग्रूमिंग प्रक्रिया में वेबकैम का उपयोग शामिल हो सकता है जिससे पीड़ित को अश्लील छवियाँ/वीडियो क्लिपिंग आदि के लिए उकसाया जा सकता है। हाल के समय में इन्टरनेट पर महिलाओं और बच्चो, के यौन शोषण के तरीके के रूप में आनलाइन ग्रूमिंग के बड़े पैमाने पर उपयोग के कारण आनलाइन ग्रूमिंग को अक्सर यौन प्रलोभन के साथ जोड़ा जाता है।

4. **साइबर स्टॉकिंग:** भारत में साइबर स्टॉकिंग की चुनौती लगातार गंभीर होती जा रही है, जिसमें महिलाओं की पीड़ितों के रूप में संख्या सर्वाधिक है। साइबर स्टॉकिंग को ऑनलाइन माध्यमों में होने वाले दुर्व्यवहार का एक स्वरूप माना जाता है, जिसके अंतर्गत इंटरनेट और डिजिटल प्लेटफॉर्म के माध्यम से किसी व्यक्ति की गतिविधियों पर "निगरानी रखना", उसका "पीछा करना" या उसे मानसिक रूप से प्रताड़ित करना शामिल होता है।

5. **ईमेल के द्वारा उत्पीड़न:** ईमेल के माध्यम से किया जाने वाला उत्पीड़न कोई नवीन परिघटना नहीं है; इसका स्वरूप पारंपरिक पत्राचार द्वारा किए जाने वाले उत्पीड़न से काफी हद तक मिलता–जुलता है। इस प्रकार के दुर्व्यवहार में ब्लैकमेलिंग, धमकियाँ देना, भय उत्पन्न करना तथा ईमेल के जरिये धोखाधड़ी जैसी गतिविधियाँ सम्मिलित होती हैं। यद्यपि ई–उत्पीड़न की प्रकृति पत्र–आधारित उत्पीड़न के समान ही होती है, किंतु फर्जी या गुमनाम ईमेल आईडी के उपयोग के कारण इसकी पहचान और नियंत्रण में व्यावहारिक कठिनाइयाँ उत्पन्न हो जाती हैं।

6. **साइबर बुलिंग:** कंप्यूटर, मोबाइल फोन, लैपटॉप जैसे इलेक्ट्रॉनिक अथवा संचार उपकरणों के माध्यम से किया जाने वाला ऐसा ऑनलाइन उत्पीड़न या डराने–धमकाने का आचरण, जिसमें यौन प्रकृति के कृत्य या संकेत सम्मिलित हों।

7. **साइबर मानहानि:** इसमें किसी व्यक्ति के विरुद्ध अपमानजनक या झूठी सामग्री को वेबसाइटों पर प्रकाशित करना अथवा उसे पीड़ित के सामाजिक और परिचित नेटवर्क में प्रसारित करना शामिल है, जिससे विशेषकर महिलाओं को गहरी मानसिक पीड़ा पहुँचती है और उनकी सामाजिक प्रतिष्ठा को क्षति होती है।

8. **ई–मेल स्पूफिंग:** यह सामान्यतः ऐसे ई–मेल को संदर्भित करता है जिसमें प्रेषक की पहचान को छिपाकर या बदलकर संदेश भेजा जाता है, मानो वह किसी विश्वसनीय स्रोत से आया हो। इस प्रकार की गतिविधियाँ आर्थिक हानि का कारण बन सकती हैं।

9. **साइबर मॉर्फिंग:** मॉर्फिंग का आशय मूल तस्वीरों में अनधिकृत रूप से संपादन करना है, जो प्रायः फर्जी पहचान या नकली प्रोफ़ाइल के माध्यम से किया जाता है। महिलाओं की तस्वीरों को डाउनलोड कर उनमें बदलाव करके झूठी प्रोफ़ाइल बनाना और विभिन्न डिजिटल प्लेटफॉर्म पर पुनः अपलोड करना इस अपराध का सामान्य स्वरूप है।

10. **साइबर फ़िशिंग:** इसमें अज्ञात अपराधियों द्वारा धोखाधड़ी के माध्यम से उपयोगकर्ता की संवेदनशील व्यक्तिगत जानकारियाँ, जैसे यूज़रनेम, पासवर्ड आदि, प्राप्त करने का प्रयास किया जाता है।

11. **साइबर ट्रोलिंग:** ट्रोल ऐसे संगठित या आदतन दुर्व्यवहारकर्ता होते हैं जो इंटरनेट पर जानबूझकर विवाद और तनाव उत्पन्न करते हैं। अश्लील या भड़काऊ सामग्री तैयार कर उसे साझा करते हुए वे महिलाओं, बच्चों और कमजोर वर्गों को भावनात्मक रूप से आहत करने और उकसाने के उद्देश्य से ऑनलाइन समुदायों में उत्तेजक पोस्ट प्रसारित करते हैं।

12. **डिजिटल अरेस्ट:** डिजिटल अरेस्ट ब्लैकमेलिंग का एक उन्नत और संगठित स्वरूप है, जिसमें अपराधी ऑनलाइन धमकियों और वीडियो कॉल के माध्यम से पीड़ित पर निगरानी रखने का भ्रम पैदा करते हैं। इस प्रक्रिया में साइबर ठग स्वयं को फर्जी पुलिस अधिकारी बताकर पीड़ितों को भयभीत करते हैं, लगातार वीडियो कॉल पर बने रहने के लिए मजबूर करते हैं और कथित मामले के निपटारे के नाम पर धनराशि ट्रांसफर करवाते रहते हैं।

इसके अलावा, यह समझने की जरूरत है कि सूचना एवं संचार प्रौद्योगिकी के विकास के कारण पारंपरिक शारीरिक अपराधों, जैसे कि बलात्कार, यौन उत्पीड़न, ब्लैकमेलिंग, पीछा करना आदि ने नया महत्त्व प्राप्त कर लिया है। बलात्कार की घटनाओं और उसके बाद मोबाइल फोन में बलात्कार के दृश्यों व तस्वीरों को सहेजकर रखने, अंतरंग पलों की तस्वीरें प्रकाशित करने की धमकी देकर पैसे ऐंठने, महिलाओं का बाद में ऑनलाइन पोर्न बाजारों के लिए उपयोग करने के लिए ग्रूमिंग, शिक्षकों द्वारा परिपक्व किशोर लड़कियों को मोबाइल फ़ोन या कंप्यूटर उपकरणों में कामोत्तेजक तस्वीरें दिखाकर शारीरिक यौन शोषण की घटनाएं भी होती हैं। डिजिटल दूरसंचार प्रणालियों के माध्यम से किए जाने वाले अपराधों के सैकड़ों उदाहरण भी मौजूद हैं जिनमें महिलाओं को अपमानजनक फोन कॉलों, SMS और MMS, इंस्टेंट मेसेजिंग सेवाओं आदि के जरिए बार–बार परेशान किया जाता है। अपराध के विभिन्न अन्य स्वरूपों नकली अवतार बनाकर "गोपनीयता का उल्लंघन", आनलाइन यौन अपराध (पोर्नोग्राफी), दर्शनरति (Voyeurism), सेक्सटिंग, इत्यादि ने महिलाओं व बच्चों को साइबर जगत में विभिन्न तरीको से पीड़ित किया है।

वैश्विक परिवेश/अन्य देशों में तकनीकी अपराधों से सम्बंधित विधियां

महिलाओं को तकनीक–आधारित अपराधों से संरक्षित करने के उद्देश्य से अंतरराष्ट्रीय स्तर पर विविध मंचों, सम्मेलनों, संधियों, बहुपक्षीय समझौतों तथा वैश्विक संस्थाओं के माध्यम से व्यापक सहयोग किया गया है। इस दिशा में बुडापेस्ट कन्वेंशन को साइबर अपराधों से निपटने हेतु स्थापित प्रथम अंतरराष्ट्रीय समझौते के रूप में माना जाता है। इसके अतिरिक्त एशिया–प्रशांत आर्थिक सहयोग (APEC), अंतरराष्ट्रीय आपराधिक पुलिस संगठन (INTERPOL), संयुक्त राष्ट्र तथा यूरोपीय संघ जैसे निकायों ने सामूहिक प्रयासों के माध्यम से साइबर अपराधों की रोकथाम हेतु नीतिगत और संस्थागत ढाँचे विकसित किए हैं। कई देशों ने इन प्रयासों को सुदृढ़ करने के लिए अपने घरेलू विधायी ढाँचों में साइबर अपराध से संबंधित विशेष प्रावधानों को सम्मिलित किया है, जिससे तकनीकी माध्यमों से होने वाले अपराधों पर प्रभावी नियंत्रण स्थापित किया जा सके। स्टॉकिंग के संदर्भ में, कैलिफोर्निया को प्रथम क्षेत्राधिकार के रूप में देखा जाता है, जिसने वर्ष 1989 में अभिनेत्री रेबेका शेफ़र की हत्या की घटना के पश्चात इस समस्या की गंभीरता को स्वीकार करते हुए स्टॉकिंग विरोधी कानून को अपनाया। इसके परिणामस्वरूप वर्ष 1990 में स्टॉकिंग को दंडनीय अपराध घोषित किया गया। इसी क्रम में न्यूयॉर्क ने भी कठोर दंडात्मक प्रावधानों को लागू करते हुए स्पष्ट किया कि स्टॉकिंग को आपराधिक कृत्य के रूप में मान्यता दी जाएगी। ऑस्ट्रेलिया ने 1993 में स्टॉकिंग क़ानून को अपनाया। साइबर स्टॉकिंग से संयुक्त राज्य अमेरिका सबसे अधिक प्रभावित देश है। संयुक्त राज्य अमेरिका ने केंद्र और राज्य स्तर पर विभिन्न कानूनों को अपनाया। पहला अधिनियम अंतरराज्यीय संचार अधिनियम है। एक अन्य संघीय कानून टेलीफोन उत्पीड़न क़ानून है। अंतरराज्यीय स्टॉकिंग दंड और रोकथाम अधिनियम। मिशिगन 1993 में अपने स्टॉकिंग कानूनों में ऑनलाइन संचार को शामिल करने वाला पहला राज्य था और

कई अन्य राज्यों ने स्टॉकिंग क़ानून को अपनाया था। 1993 में मिशिगन आपराधिक संहिता ने पहली बार साइबर स्टॉकिंग सहित स्टॉकिंग को अपराध घोषित किया था। 'अमेरिकी क़ानूनों द्वारा साइबर स्टॉकिंग को 'उत्पीड़न' माना गया था, जिसने 'उत्पीड़न' शब्द को 'पीड़ित के प्रति निर्देशित ऐसे आचरण' के तौर पर परभाषित किया था जिसमें बार–बार या सहमति के बिना संपर्क शामिल है जिसके कारण विचारपूर्ण व्यक्ति को भावनात्मक पीड़ा का सामना करना पड़े और जिसके कारण वास्तव में पीड़ित को भावनात्मक पीड़ा का सामना करना पड़ता है। "मिशिगन आपराधिक संहिता ने आगे बताया कि 'सहमति के बिना संपर्क' का अर्थ 'पीड़ित को अनचाहे और अवांछित मेल या इलेक्ट्रॉनिक संचार भेजना' हो सकता है। वर्तमान में संयुक्त राज्य अमेरिका के कई प्रांतों ने साइबर स्टॉकिंग विरोधी क़ानूनों को लागू किया है जो साइबर स्टॉकिंग को उत्पीड़न के समान संकेतार्थ में समझाते हैं। वायलेंस अगेंस्ट वीमेन एंड डिपार्टमेंट ऑफ़ जस्टिस रीऑथोराइज़ेशन एक्ट, 2005, जिसने धारा 114 के माध्यम से शीर्षक 18, USC की धारा 2261A को संशोधित किया, के आने साथ साइबर स्टॉकिंग की अवधारणा को और स्पष्ट रूप से समझाया गया था। 'साइबर स्टॉकिंग' शब्द को अभी भी युनाइटेड किंग्डम में किसी विशेष क़ानूनी प्रावधान द्वारा परिभाषित नहीं किया गया है। उत्पीडन से सुरक्षा अधिनियम (PHA), 198715 के Ss-2–7 सहित प्रावधानों को वर्तमान में स्टॉकिंग और साइबर स्टॉकिंग के लिए नियामक प्रावधान के रूप में उपयोग किया जाता है। हालांकि PHA 'साइबर स्टॉकिंग' शब्द को विशेष रूप से परिभाषित नहीं करता है परंतु क्राउन प्रोसेस्यूशन सर्विस (CPS), S2A(3) की रूपरेखा के आधार पर साइबर स्टॉकिंग की एक विस्तृत परिभाषा प्रदान करता है। इसके अनुसार, उत्पीड़न इंटरनेट पर एवं ईमेल के दुरुपयोग के माध्यम से हो सकता है। इसे कभी–कभी 'साइबर स्टॉकिंग' के रूप में जाना जाता है। इसमें सोशल नेटवर्किंग साइट्स, चौट रूम और प्रौद्योगिकी द्वारा सुविधा प्राप्त अन्य मंचों का उपयोग शामिल हो सकता है। इंटरनेट का उपयोग उत्पीड़न से संबंधित कई उद्देश्यों के लिए किया जा सकता है, उदाहरण के लिए: पीड़ित के बारे में व्यक्तिगत जानकारी का पता लगाना; पीड़ित के साथ संवाद करना; पीड़ित की निगरानी के साधन के रूप में; पहचान की चोरी जैसे कि पीड़ित को सेवाओं की सदस्यता देना, उनके नाम पर माल और सेवाएं खरीदना; पीड़ित की प्रतिष्ठा को नुकसान पहुंचाना; इलेक्ट्रॉनिक गड़बड़ी जैसे कि स्पैमिंग और वायरस भेजना; या अन्य इंटरनेट उपयोगकर्ताओं को चलाकी से पीड़ित का उत्पीड़न करने या धमकाने में शामिल करना।" साइबर–स्टॉकिंग से निपटने के लिए यूके के पास कोई विशिष्ट कानून नहीं है। ऐसे तीन कानून हैं जो इस तरह के व्यवहार को अपराधी बनाने का प्रयास करते हैं। इनमें से पहला कानून दूरसंचार अधिनियम, 1984 है। इस अधिनियम के तहत, दूरसंचार प्रणाली के माध्यम से ऐसा संदेश भेजना अपराध है जो "बेहद आक्रामक या अभद्र, अश्लील या धमकी देने वाला चरित्र" हो या "परेशानी, असुविधा या अनावश्यक चिंता पैदा करने" के उद्देश्य से संदेश हो और यह जानते हुए भी कि संदेश झूठा है। दूसरा कानून उत्पीड़न से सुरक्षा अधिनियम, 1997 है, जो आपराधिक उत्पीड़न के अपराध और हिंसा के डर से जुड़े अपराध को सिविल और आपराधिक उपायों के अधीन बनाता है। तीसरा कानून दुर्भावनापूर्ण संचार अधिनियम, 1988 है जिसमे आपराधिक न्याय और पुलिस अधिनियम, 2001 द्वारा, इस कानून में इलेक्ट्रॉनिक संचार को भी शामिल करने के लिए संशोधन किया गया था।

तकनीकी अपराधों से सम्बंधित भारतीय विधियां

1. **भारत का संविधान, 1950:** अनुच्छेद 19 और 21 महिलाओं बच्चों और कमजोर वर्गों को तकनीकी आधारित अपराधों से सुरक्षा प्रदान करता है। संविधान का अनुच्छेद 19(1) (ए) भाषण और अभिव्यक्ति का मौलिक अधिकार प्रदान करता है। यह अधिकार निरपेक्ष नहीं है और अनुच्छेद 19(2) के तहत उल्लिखित उचित प्रतिबंधों के अधीन है। और संविधान का अनुच्छेद 21 भारत में महिलाओं बच्चों और कमजोर वर्गों को साइबर स्पेस में मानवीय गरिमा के साथ रहने का अधिकार देता है।

2. **सूचना प्रौद्योगिकी अधिनियम, 2000:** आईटी अधिनियम, 2000 के अंतर्गत धाराएँ हैं 66A संचार सेवा के माध्यम से आपत्तिजनक संदेश भेजने के लिए, धारा 65 कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़ करने के लिए, धारा 70 गोपनीय जानकारी के साथ छेड़छाड़ करने के लिए, धारा 72 ऑनलाइन स्टॉकिंग के लिए, धारा 42A और धारा 66 आईटी अधिनियम, 2000 (आईपीसी, 1860 की धारा 379, 406 के साथ) डेटा हैकिंग के लिए, धारा 43B, 66E और 67C डेटा चोरी के लिए, धारा 67A पोर्नोग्राफी के लिए।

3. **कॉपी राइट अधिनियम, 1957:** कॉपी राइट अधिनियम, 1957 की धारा 63B महिलाओं को डेटा चोरी से सुरक्षा प्रदान करती है। इस धारा के अंतर्गत यह प्रावधान किया गया है कि कोई भी व्यक्ति जो जानबूझकर कंप्यूटर या कंप्यूटर प्रोग्राम की उल्लंघनकारी कॉपी का उपयोग करता है, उसे दंड दिया जाएगा।

4. **यौन अपराधों से बच्चों का संरक्षण (POCSO) अधिनियम, 2012:** POCSO अधिनियम, 2012 बच्चों/बालिकाओं को सुरक्षा प्रदान करता है, इसके अंतर्गत प्रावधान हैं– पेनेट्रेटिव यौन हमले के लिए धारा 3, गंभीर पेनेट्रेटिव यौन हमले के लिए धारा 5, यौन हमले के लिए धारा 7, गंभीर यौन हमले के लिए धारा 9, बच्चे के यौन उत्पीड़न के लिए धारा 11, पोर्नोग्राफिक उद्देश्यों के लिए बच्चे के उपयोग के लिए धारा– 13

5. **भारतीय न्याय सहिंता, 2023:** भारतीय न्याय सहिंता– 2023 को दंड सहिंता 1860 के स्थान पर पुनर्स्थापित किया गया है। जिसमे सम्बंधित प्रावधान धारा– 74, 75,76,77, 78, 79, 294, 295,296, 351 352 है।

यद्यपि कि भारत का संविधान महिलाओं को जीवन के समान अधिकार, मानवीय सम्मान के साथ जीने का अधिकार और भाषण और अभिव्यक्ति के अधिकार की गारंटी देता है, लेकिन महिलाओं की समान विनम्रता को सामान्य रूप से सूचना प्रौद्योगिकी अधिनियम, 2000 में संरक्षित नहीं किया गया है। आईटी अधिनियम, 2000 में कोई विशिष्ट प्रावधान नहीं हैं जो विशेष रूप से महिलाओं के खिलाफ अपराध से निपटते हैं इसी प्रकार, POCSO, 2012 भी बच्चों के विरुद्ध साइबर अपराधों को रोकने में पूरी तरह सक्षम नहीं है। इसी तरीके से सूचना प्रौद्योगिकी अधिनियम, 2000 और भारतीय न्याय संहिता, 2023 में साइबरस्टॉकिंग और ऑनलाइन वित्तीय धोखाधड़ी जैसे डिजिटल युग के अपराधों से निपटने के लिए व्यापक प्रावधानों का अभाव है।

तकनीकी के दौर में महिलाओं बच्चों और कमजोर वर्गों के विरुद्ध बढ़ते अपराध: न्यायिक प्रवृत्तियां

विधायिका एवं न्यायपालिका राज्य व्यवस्था के दो महत्वहपूर्ण अंग है। विधायिका जहां विधि निर्माण की सर्वोच्च संस्था हैं तो वहीं न्यायपालिका राष्ट्र की मूल विधि (संविधान) की संरक्षक एवं नागरिकों के अधिकारों की रक्षा करने वाली सजग प्रहरी है। इन

दोनो ही संस्थाओं के बिना राष्ट्र संचालन सम्भव नहीं है। यदि "महिलाओं बच्चों और कमजोर वर्गों के विरुद्ध तकनीकी आधारित अपराधों से उन्मूलन हेतु" हम इन अंगों का अवलोकन करें तो पायेंगे कि यदि ये दोनो अंग तकनीकी आधारित अपराधों के उन्मूलन हेतु अपने कर्तव्यों एवं शक्तियों का सार्थक प्रयोग करें तो तकनीकी आधारित अपराध के पूर्ण रुप से उन्मूलन का लक्ष्य सही मायनों में प्राप्त करना असम्भव न होगा, किन्तु वास्तविक स्थिति इस विचार को पूर्णतया चरितार्थ नहीं करती है। इसी विचार को केन्द्र में रखते हुए महिलाओं बच्चों और कमजोर वर्गों के विरुद्ध तकनीकी आधारित अपराधों के पूर्ण रुप से उन्मूलन में न्यायपालिका की भूमिका का वस्तु स्थिति वर्णन अग्रलिखित है–

रंजीत डी. उदेशी बनाम महाराष्ट्र यह भारत में साइबर अश्लीलता पर आधारित वाला पहला बड़ा मामला है। 19वीं सदी के दौर में लंदन में एक कोर्ट रिकॉर्डर था। उसका नाम बेंजामिन फ्रैंकलिन था और उसके नाम पर ही इस टेस्ट का नाम "हिकलिन टेस्ट" रखा गया। मूल रूप से, यह एक अश्लीलता मानक है, जिसकी उत्पत्ति एक अंग्रेजी मामले– रेजिना बनाम हिकलिन (1868) से हुई थी, यह मामला महिला पोर्नोग्राफी और अश्लीलता पर आधारित है, इस मामले में हिकलिन टेस्ट नामक एक प्रतिपादित सिद्धांत महिला पोर्नोग्राफी के संदर्भ में अश्लीलता का एक मानक है। हालांकि बाद में अवीक सरकार बनाम पश्चिम बंगाल राज्य के वाद में सुप्रीम कोर्ट ने सामुदायिक मानक परीक्षण के पक्ष में हिकलिन परीक्षण को खारिज कर दिया। बाद के परीक्षण में आपत्तिजनक भागों को अलग करने के बजाय पूरे काम और उसके संदर्भ पर विचार किया गया, जिससे अश्लीलता और यौन सामग्री के प्रति विकसित होते सामाजिक दृष्टिकोण को दर्शाया गया।

वर्ष 2002 में, तमिलनाडु राज्य बनाम डॉ एल प्रकाश, यह मामला सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 67 के तहत इलेक्ट्रॉनिक रूप में अश्लील सामग्री प्रसारित करने के अपराध के संबंध में दंडित करने वाला भारत का पहला मामला है। सेक्स डॉक्टर' एल. प्रकाश के मामले, जिसे उसके फार्म हाउस में बंद लड़कियों की अश्लील तस्वीरें लेने और उन्हें इंटरनेट पर पोस्ट करने के लिए 2001 में महिलाओं के अश्लील निरूपण (रोकथाम) अधिनियम के विभिन्न प्रावधानों, अनैतिक तस्करी (रोकथाम) अधिनियम और मुख्य रूप से IT अधिनियम की धारा 67 के तहत आरोपित और गिरफ्तार किया गया था और मद्रास में निचली अदालत द्वारा 2008 में लिए गए फैसले में आजीवन कारावास की सज़ा सुनाई गई थी। लेकिन बाद में मद्रास उच्च न्यायालय द्वारा आजीवन कारावास की सज़ा में बदलाव करने के बाद उसे विमुक्त कर दिया गया था क्योंकि वह पहले ही 13 वर्षों की सज़ा काट चुका था।' जैसा कि पूर्व मामलों में देखा गया है, साइबर पोर्नोग्राफी और अश्लीलता की क़ानूनी अवधारणा अदालतों द्वारा अच्छी तरह से विकसित या उचित ढंग से निष्पादित नहीं की गई थी। हालांकि, अब इस संदर्भ में सकारात्मक सुधार हुए हैं।

मनीष कथूरिया बनाम रितु कोहली वर्ष 2001 में भारत में पहली बार साइबर स्टॉकिंग का मामला सामने आया था। मनीष कथूरिया एक भारतीय महिला, सुश्री रितु कोहली को उनके नाम का उपयोग करके www.mirc.com वेबसाइट पर अवैध रूप से चौट करके पीछा कर रहा था; और अश्लील और अप्रिय भाषा का इस्तेमाल कर रहा था, और उनके निवास का टेलीफोन नंबर वितरित कर लोगों को फोन पर उनके साथ चौट करने के लिए आमंत्रित कर रहा था। नतीजतन, सुश्री रितु कोहली को भारत के विभिन्न राज्यों और विदेशों से अश्लील कॉल आ रहे थे। पुलिस ने रितु कोहली की गरिमा को ठेस पहुंचाने के आरोप में भारतीय दंड संहिता, 1860 की धारा 509 के तहत मामला दर्ज किया। लेकिन धारा 509 केवल एक शब्द, एक इशारा या एक कृत्य को संदर्भित करती है जिसका उद्देश्य किसी के साथ दुर्व्यवहार करना है। किसी महिला की गरिमा का अपमान करना। लेकिन जब यही काम इंटरनेट पर किया जाता है, तो इस धारा में इसका कोई उल्लेख नहीं होता। इस मामले ने भारत सरकार को इस बात के लिए सचेत किया कि उपरोक्त अपराध के संबंध पीड़ितों की सुरक्षा के लिए कानूनों में संशोधन करने की आवश्यकता है। इसलिए, 2008 में भारत की संसद ने आईटी अधिनियम 2000 में संशोधन किया और साइबर स्टॉकिंग के लिए प्रावधान किए। आईटी अधिनियम, 2008 सीधे स्टॉकिंग को संबोधित नहीं करता है। लेकिन इस समस्या को आईटी अधिनियम, 2008 में चर्चा किए गए नियमित साइबर अपराधों की तुलना में "व्यक्ति की गोपनीयता में घुसपैठ" के रूप में अधिक लिया जाता है। इसलिए भारत में साइबर स्टॉकिंग को विनियमित करने के लिए सबसे अधिक इस्तेमाल किया जाने वाला प्रावधान आईटी अधिनियम, 2008 की धारा 72 है।

सर्वोच्च न्यायालय का एक महत्वपूर्ण मामला श्रेया सिंघल बनाम भारत संघ, यह मामला सोशल मीडिया पर महिलाओं के खिलाफ साइबर अपराध से सुरक्षा के नवीनतम मामलों में से एक है जो साइबरस्पेस में महिलाओं के लिए खतरा है, अभिव्यक्ति की स्वतंत्रता की रक्षा करता है, इस मामले में, सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 66ए (2008 में संशोधन के माध्यम से सम्मिलित) को सर्वोच्च न्यायालय ने असंवैधानिक करार दिया था। न्यायालय ने यह ऐतिहासिक फैसला तब लिया जब याचिका में आरोप लगाया गया कि उक्त प्रावधान बेहद अस्पष्ट है, लेकिन जबकि यह स्वीकार किया जाता है कि प्रावधान एक कठोर कानून हो सकता है? क्या सर्वोच्च न्यायालय इस अवसर का उपयोग कुछ प्रकार के भाषण को विनियमित करने के प्रावधान को फिर से तैयार करने और पुन: प्रस्तुत करने के लिए कर सकता है, जिसे इंटरनेट पर "बुरी बात" कहा जा सकता है? यह ध्यान दिया जा सकता है कि भारत में साइबर बदमाशी और ट्रोलिंग, ऑनलाइन लिंग उत्पीड़न, तोड़फोड़ और विशिंग बड़े पैमाने पर हो रहे हैं। न्यायालय बेहतर कानून बनाने के लिए धारा –66A के चिकित्सीय न्यायशास्त्रीय मूल्य पर विचार कर सकता था।

वर्ष 2004 में तमिलनाडु राज्य बनाम सुहास कुट्टी का मामला प्रकाश में आया। इस मामले में, अतिरिक्त मुख्य मेट्रोपोलिटन मजिस्ट्रेट ने आरोपी को सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 67 और भारतीय दंड संहिता, 1860 की धाराओं 469 और 509 के अंतर्गत दोषी ठहराया। आरोपी सुहास कट्टी को दोषी ठहराया गया और सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 67 के अंतर्गत 4,000 रुपए के जुर्माने के साथ दो वर्ष के कठोर कारावास, भारतीय दंड संहिता की धारा 469 के अंतर्गत 500 रुपए के जुर्माने के साथ दो वर्ष के कठोर कारावास और भारतीय दंड संहिता की धारा 509 के अंतर्गत 500 रुपए के जुर्माने के साथ एक वर्ष के साधारण कारावास की सजा सुनाई गई। तमिलनाडु राज्य बनाम सुहास कट्टी का मामला भारत में साइबर कानूनों के प्रवर्तन में एक कानूनी मिसाल के रूप में काम करता है और महिलाओं के खिलाफ साइबरस्टॉकिंग और अन्य ऑनलाइन अपराधों से निपटने के लिए न्यायपालिका की प्रतिबद्धता को उजागर करता है। इसने साइबर उत्पीड़न के पीड़ितों को आगे आने और अपराधों की रिपोर्ट करने के लिए प्रोत्साहित किया, यह जानते हुए कि कानूनी प्रणाली उनके अधिकारों की रक्षा करेगी और अपराधियों के खिलाफ कार्रवाई करेगी।

कमलेश वासवानी बनाम भारतीय संघ एवं अन्य के मामले का उल्लेख इस सन्दर्भ में यहाँ अवश्य किया जाना चाहिए। इस मामले में याचिकाकर्ता द्वारा दायर की गई जनहित याचिका (PIL) में यह उल्लेख किया गया था कि पोर्नोग्राफी क़ानून में एक कमी थी जिसके कारण भारतीय समाज में अत्यधिक अश्लील वीडियो का प्रवेश हुआ और इससे युवाओं, खासकर बच्चों को

गंभीर नुकसान पहुंचा है। ऐसे सामाजिक विचार हैं कि पोर्नोग्राफी देखना एक तरीके से समाज में यौन अपराधों, खासकर बलात्कार, महिलाओं व लड़कियों के यौन उत्पीडन और पाशविकता को प्रेरित करता है। यही राय उपर्यक्त मामले में भी व्यक्त की गई थी। यह एक दर्भाग्यपूर्ण तथ्य है कि भारत के कानूनों ने इलेक्ट्रॉनिक माध्यमों से कामोत्तेजक सामग्रियों द्वारा पोर्नोग्राफी के प्रकाशन, प्रसारण या पोर्नोग्राफिक सामग्री बनाने के लिए बच्चों के उपयोग को स्पष्ट रूप से अपराध घोषित किया है लेकिन वयस्कों द्वारा गुप्त रूप में पोर्नोग्राफी देखने पर प्रतिबंध लगाने के लिए कोई क़ानून नहीं है।

विनय कुमार एवं अन्य बनाम महाराष्ट्र सरकार के मामले में बंबई उच्च न्यायालय का फैसला इस संबंध में उल्लेखनीय है। इस मामले में बंबई उच्च न्यायालय ने कहा कि किसी व्यक्ति द्वारा अपने निजी निवास की चारदीवारी के अंदर पोर्नोग्राफिक सामग्रियां देखना कोई अपराध नहीं है खासकर जब यह सामग्रियां, डिजिटल रूप, सीडी आदि के द्वारा बिक्री, किराये पर देने, वितरण आदि के लिए नहीं हैं।

राष्ट्रपति प्रणब मुखर्जी की बेटी का पीछा करने का मामला राष्ट्रपति प्रणब मुखर्जी की बेटी शर्मिष्ठा मुखर्जी को कथित तौर पर एक व्यक्ति ने परेशान किया, जिसने उनके फेसबुक पेज पर यौन रूप से स्पष्ट संदेश पोस्ट किए। उन्होंने दिल्ली पुलिस की साइबर अपराध इकाई में शिकायत दर्ज कराई। पुलिस ने कहा कि शिकायतकर्ता को फेसबुक मैसेंजर के माध्यम से "अश्लील" संदेश भेजे गए थे। प्रेषक की प्रोफ़ाइल में उसे पश्चिम बंगाल के हुगली में नौहाटी का निवासी बताया गया है। मुखर्जी ने उन्हें भेजे गए संदेशों के स्क्रीनशॉट साझा किए और कहा कि उन्होंने ऑनलाइन उत्पीड़न के खिलाफ़ बोलने का फैसला किया क्योंकि इसे अनदेखा करने से वह और भी प्रोत्साहित होगा। उन्होंने उस व्यक्ति को भी टैग किया जिसने अब फेसबुक से अपना प्रोफ़ाइल हटा दिया है। उन्होंने फेसबुक पर पोस्ट किया कि "यह विकृत व्यक्ति पार्थ मंडल मुझे गंदे यौन संदेश भेज रहा है। मेरी पहली प्रतिक्रिया उसे अनदेखा करना और ब्लॉक करना था। लेकिन फिर मैंने सोचा कि चुप्पी उसे अन्य पीड़ितों को खोजने के लिए प्रोत्साहित करेगी। केवल ब्लॉक करना और रिपोर्ट करना पर्याप्त नहीं है। मुझे दृढ़ता से लगता है कि ऐसे लोगों को सार्वजनिक रूप से उजागर किया जाना चाहिए और अपमानित किया जाना चाहिए। मैं उसकी प्रोफ़ाइल और उसके द्वारा मुझे भेजे गए संदेशों के स्क्रीनशॉट पोस्ट कर रही हूँ। मैं उसे टैग भी कर रही हूँ। कृपया इस पोस्ट को शेयर करें और इस चूहे को एक संदेश के रूप में टैग करें कि इन विकृत कृत्यों को हल्के में नहीं लिया जाएगा।, "

निष्कर्ष

इक्कीसवीं सदी के सबसे महत्वपूर्ण आविष्कारों में से एक इंटरनेट आधुनिक दुनिया के लिए एक बड़ा खतरा बन गया है। इसमें कोई संदेह नहीं है कि इंटरनेट के विकास ने मानव को नवाचार करने का अवसर बढ़ाया है, लेकिन इसने मानव खतरे को भी बढ़ाया है। हममें से लगभग सभी लोग कंप्यूटर, मोबाइल फोन और अन्य प्रकार के संचार उपकरण, नेटवर्क और इंटरनेट का उपयोग करते हैं। यह बिना कहे ही स्पष्ट है कि सबसे कठिन और महत्वपूर्ण मुद्दा साइबर अपराध करने वाले बच्चों से संबंधित है। यह सर्वविदित है कि कई अमीर देश साइबर अपराध करने वाले युवाओं से निपटने के लिए संघर्ष करते हैं। भारत में भी बच्चों से जुड़े कई साइबर अपराध दर्ज किए गए हैं। नतीजतन, यह अध्ययन भारत में उच्च ऑनलाइन प्रवृत्ति, साइबर विचलन और महिलाओं और बच्चों को साइबर अपराधों से बचाने में अदालतों की भूमिका से संबंधित चर और डेटा की एक महत्वपूर्ण समीक्षा है। डिजिटल युग में, प्रौद्योगिकी में तेजी से हुई प्रगति ने हमारे जीने, काम करने और एक–दूसरे के साथ बातचीत करने के तरीके को बदल दिया है। इन प्रगतियों ने जहाँ कई लाभ लाए हैं, वहीं उन्होंने नई चुनौतियों को भी जन्म दिया है, खासकर साइबर सुरक्षा के क्षेत्र में। साइबर अपराध, जिसमें डिजिटल चौनलों के माध्यम से की जाने वाली कई तरह की अवैध गतिविधियाँ शामिल हैं, एक व्यापक खतरा बन गया है जो दुनिया भर में व्यक्तियों, व्यवसायों और समाजों को प्रभावित करता है। अगर आकड़ों की बात की जाए तो भारत में साइबर क्राइम रिपोर्ट 2022 के अनुसार, साइबर अपराध के तहत कुल 65,893 मामले तथा वर्ष 2021 में 52,974 मामले दर्ज किए गए। जो तुलना में 24.4% की वृद्धि दर्शाता है। खराब आंकड़ों के लिए कुछ हद तक दोष इस तथ्य में भी है कि हमारे पास पर्याप्त कानून नहीं हैं। लिंग आधारित साइबर हिंसा (जी0बी0सी0वी0) के कई प्रकारों को कानून द्वारा नजरअंदाज कर दिया जाता है, और हमें अंततः अश्लीलता–विरोधी प्रावधानों पर निर्भर रहना पड़ता है। स्त्री–द्वेष में डूबे, अश्लीलता–विरोधी प्रावधान महिलाओं की यौन अभिव्यक्ति की उपेक्षा करते हैं और राज्य को महिलाओं के शरीर की निगरानी करने का अधिकार देते हैं, यदि वह उनके प्रतिनिधित्व को "अशिष्ट" मानता है। सूचना प्रौद्योगिकी, 2000 में धारा 66E जैसे अन्य अधिक प्रगतिशील विकल्प हैं; हालाँकि, इस धारा का शायद ही उपयोग किया जाता है । भारत में अभी भी लिंग आधारित अभद्र भाषा पर कोई कानून नहीं है। देश में अभद्र भाषा कानूनों को संशोधित करने के लिए गठित विधि आयोग और टीके विश्वनाथन समिति ने व्यापक और अस्पष्ट शब्दों में बदलाव का सुझाव दिया है, जिसकी आलोचना की गई है यदि इसे कानून में शामिल कर लिया जाए, तो महिलाएं अश्लीलता आधारित प्रावधानों पर निर्भर हुए बिना, ऑनलाइन लैंगिक भेदभाव और यौन उत्पीड़न करने वालों के खिलाफ कार्रवाई कर सकेंगी, जिन्हें चरणबद्ध तरीके से समाप्त किया जाना चाहिए। भारतीय परिदृश्य में महिलाओं, बच्चों और कमजोर वर्गों के विरुद्ध तकनीकी आधारित अपराधों के मामले तेजी से बढ़ रहे हैं, जिनमें साइबर ट्रोलिंग और साइबर बुलिंग जैसे नए अपराध शामिल हैं। लेकिन आईटी एक्ट, 2000 में ऐसे अपराधों को शामिल नहीं किया गया है और जांच की प्रक्रिया भी उचित नहीं है। साइबर टोलिंग और जेंडर बुलिंग के लिए एक्ट में कोई उपाय नहीं दिया गया है, जो एक्ट की कमियों में से एक है। इसी तरह साइबर स्टॉकिंग भी एक गंभीर अपराध है, जिससे निपटने के लिए आईटी एक्ट, 2000 में संशोधन करके सख्त कानून बनाने की जरूरत है और अधिकांश साइबर अपराधों को गैर–जमानती अपराध बनाने की जरूरत है। जांच के लिए अलग सेल बनाने की जरूरत है और एक अलग कानून बनाने की जरूरत है। कानून को और अधिक प्रभावी बनाने के लिए इसमें व्यापक डेटा सुरक्षा व्यवस्था को शामिल करने की जरूरत है। महिलाओं के खिलाफ साइबर अपराध से निपटने के लिए अधिकारियों को विशेष प्रशिक्षण दिया जाना चाहिए। और भारत में महिलाओं के खिलाफ हो रहे साइबर अपराध को रोकने के लिए भारत की न्यायपालिका को महत्वपूर्ण योगदान देना होगा। भारत सरकार को साइबर अपराध पर सूचनाओं के आदान–प्रदान के लिए अन्य देशों के साथ द्विपक्षीय सहयोग की दिशा में काम करना चाहिए। हाल ही में औपनिवेशिक युग के कानूनों से भारतीय न्याय संहिता और भारतीय नागरिक सुरक्षा संहिता में बदलाव किया गया है। फिर भी नई संहिता में साइबरस्टॉकिंग और ऑनलाइन वित्तीय धोखाधड़ी जैसे डिजिटल युग के अपराधों से निपटने के लिए व्यापक प्रावधानों का अभाव है, जिनकी आज के तकनीकी रूप से संचालित समाज में प्रासंगिकता तीव्रता से बढ़ रही है। सामाजिक और सांस्कृतिक संवेदनशीलता के प्रति भारतीय न्याय सहिंता– 2023 का दृष्टिकोण अतिरिक्त खतरे की घंटी बजाता है। महिलाओं की सुरक्षा के लिए प्रावधान पेश करने के बावजूद, लिंग–पक्षपाती भाषा और वैवाहिक बलात्कार अपवाद को बनाए रखना निश्चित रूप से परेशान करने वाला है। ये

पहलू लैंगिक रूढ़िवादिता को बनाए रखते हैं और यौन अपराधों के सभी पीड़ितों को व्यापक सुरक्षा प्रदान करने में विफल रहते हैं। इन मुद्दों को पूरी तरह से संबोधित करने में कानून की विफलता वास्तविक लैंगिक समानता के प्रति प्रतिबद्धता की कमी को दर्शाती है। इसमें सभी प्रासंगिक धाराओं में लिंग–तटस्थ भाषा को शामिल करना चाहिए, जिससे यौन अपराधों के सभी पीड़ितों के लिए व्यापक सुरक्षा सुनिश्चित हो सके। वैवाहिक बलात्कार अपवाद पर पुनर्विचार और संशोधन करना विवाह के भीतर महिलाओं को पूर्ण सुरक्षा प्रदान करने के लिए महत्वपूर्ण है, जो अंतरराष्ट्रीय मानवाधिकार मानकों के अनुरूप है। इसके अलावा, भारतीय न्याय सहिंता– 2023 में डिजिटल डिवाइड को पाटने के उपाय शामिल होने चाहिए। इसे देशव्यापी डिजिटल साक्षरता कार्यक्रमों में निवेश करके और डिजिटल बुनियादी ढांचे में सुधार करके हासिल किया जा सकता है, खासकर ग्रामीण और वंचित क्षेत्रों में। प्रौद्योगिकी तक समान पहुंच सुनिश्चित करने से कमजोर और हाशिए पर पड़े समुदायों को कानूनी रूप से वंचित होने से रोका जा सकेगा। बीएनएस के नए प्रावधानों और तकनीकी पहलुओं पर कानून प्रवर्तन अधिकारियों के लिए व्यापक प्रशिक्षण कार्यक्रम महत्वपूर्ण हैं। इसके अतिरिक्त, इन प्रशिक्षण कार्यक्रमों के प्रभावी कार्यान्वयन को सुनिश्चित करने के लिए नियमित निगरानी और मूल्यांकन तंत्र स्थापित किए जाने चाहिए।

सन्दर्भ ग्रन्थ सूची

1. नेहा चौधरी, नारी देह के विरुद्ध हिंसा, संस्करण–2020, सेज प्रकाशन नई दिल्ली
2. के जयशंकर, देबारती हालदर, भारत में महिलाओं के विरुद्ध साइबर अपराध, संस्करण 2019, सेज पब्लिकेशन नई दिल्ली
3. Halder D, Jaishankar K (June 2011). Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. Page-131.
4. Schrock A, Boyd D, (2008). Online threats to youth: Solicitation, harassment, and problematic content. Final report of the internet safety technological task force. Enhancing Child Safety and Online Technologies.
5. Halder D. (2015) Cyber stalking victimisation of women: Evaluating the effectiveness of current laws in India from restorative justice and therapeutic jurisprudential perspectives- TEMIDA, 18(3-4), 103-130: doi:10.2298/TEM1504103H News Articles & Blogs
6. https://www-cyberpeace-org/resources/blogs/emerging-cyber-crime-hotspots
7. https://www-thehindu-com/news/national/crimes-against-women-children-scst-and-cyber-crimes-increased-in-2022-crime-in-india-report/article67602315-ece
8. https://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india
9. https://hindi-news18-com/news/nation/pranab-mukherjees-daughter-sharmistha-mukherjee-gets-seÛually-harassed-online-902506.html
10. http://www.thehindu.com/news/cities/chennai/convict-in-cyber-porn-case-released/article7142399.ece
11. http://www.thehindu.com/news/national/other-states/bihar-police-giving-repeated-missed-call-to-women-is-stalking-attracts-jail-term/article64422863.ece
12. https://www.hindustantimes.com/delhi/delhi-metro-video-of-intimate-couple-leaked-again/story-mACÛWcec0JHcjIIrrF5M7K.html
13. https://thehackernews.com/2015/04/net-neutrality-trai-emails.html Government & Legal Resources
14. https://www.mass.gov/info-details/know-the-types-of-cyber-threats
15. http://www.legislation.gov.uk/ukpga/1997/40/contents
16. https://www.cps.gov.uk/prosecution-guidance/stalking-or-harassment
17. http://www.haltabuse.org/resources/laws/michigan.shtml
18. https://lawbhoomi.com/cyber-defamation/
19. https://www.sanskritiias.com/hindi/current-affairs/digital-arrest-2
20. https://www.proofpoint.com/us/threat-reference-cyber-crime
21. भारत का संविधान, 1950
22. सूचना प्रौद्योगिकी अधिनियम–2000
23. सूचना प्रौद्योगिकी (संशोधन) अधिनियम–2008
24. कॉपी राइट अधिनियम, 1957
25. यौन अपराधों से बच्चों का संरक्षण (POCSO) अधिनियम, 2012
26. भारतीय न्याय सहिंता– 2023
27. धारा 43, दूरसंचार अधिनियम, 1984
28. एसएस 2(2),4(4) उत्पीड़न से संरक्षण अधिनियम, 1997
29. धारा 1– दुर्भावनापूर्ण संचार अधिनियम, 1988,
30. धारा 43– आपराधिक न्याय और पुलिस अधिनियम, 2001, Case Laws
31. रंजीत डी. उदेशी बनाम महाराष्ट्र आपराधिक अपील संख्या 178 / 1962 निर्णय तिथि– 19 अगस्त 1964
32. अवीक सरकार बनाम पश्चिम बंगाल राज्य (2014) 4 एससीसी 257
33. कमलेश वासवानी बनाम भारतीय संघ एवं अन्य रिट याचिका (सिविल) सं. 177 / 2013
34. रेजिना बनाम हिकलिन (1868)
35. तमिलनाडु राज्य बनाम डॉ एल प्रकाश रिट याचिका संख्या 7313 / 2002 और WPMP संख्या 10120 / 2002
36. मनीष कथूरिया बनाम रितु कोहली
37. श्रेया सिंघल बनाम भारत संघ रिट याचिका संख्या 167 / 2012 निर्णय तिथि 24 मार्च– 2015
38. तमिलनाडु राज्य बनाम सुहास कुट्टी केस नम्बर 4680 / 2004 निर्णय तिथि– 5 नवम्बर– 2004
39. विनय कुमार एवं अन्य बनाम महाराष्ट्र सरकार आपराधिक आवेदन सं. 2809 / 2010