The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 11 | November 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

साइबर अपराध में महिला पीड़ितों के लिए डिजिटल साक्ष्य का महत्व

Ankita Keshri

Research Scholar, Department of Law, NIILM University, Kaithal, Hariyana

Email: ankita.keshri24@gmail.com

Dr. Sayyad Ismail Nasir

Research Guide, Department of Law, NIILM University, Kaithal, Hariyana

DOI : https://doi.org/10.5281/zenodo.17922493

ARTICLE DETAILS

Research Paper

Accepted: 22-11-2025

Published: 10-12-2025

Keywords:

साइबर अपराध, महिला पीड़िता, ऑनलाइन उत्पीड़न, डिजिटल साक्ष्य

ABSTRACT

डिजिटल युग ने समाज को नई दिशा दी है और जीवन को अभूतपूर्व सुविधाओं से संपन्न बनाया है। इंटरनेट और सोशल मीडिया ने जहाँ संचार, शिक्षा और अवसरों का नया संसार खोला है, वहीं इसके दुरुपयोग ने गंभीर चुनौतियाँ भी उत्पन्न की हैं। विशेषकर महिलाओं के विरुद्ध होने वाले साइबर अपराध इस आधुनिक तकनीकी युग का सबसे संवेदनशील और चिंताजनक पहलू हैं। साइबर स्टॉकिंग, मॉर्फिंग, निजी तस्वीरों और वीडियो का दुरुपयोग, सोशल मीडिया के माध्यम से उत्पीड़न, धमकी, और फर्जी पहचान बनाकर शोषण जैसे अपराध महिलाओं की गरिमा और स्वतंत्रता पर सीधा आघात करते हैं। इन अपराधों की विशेषता यह है कि इनका स्वरूप भौतिक नहीं, बल्कि आभासी होता है। अपराधी अक्सर दूर बैठे रहते हैं और डिजिटल प्लेटफ़ॉर्म का सहारा लेकर अपनी गतिविधियों को अंजाम देते हैं। ऐसे में अपराध को साबित करने और दोषी को न्यायालय तक पहुँचाने में सबसे बड़ी भूमिका डिजिटल साक्ष्य निभाते हैं। मोबाइल फोन, ईमेल, चैट हिस्ट्री, सोशल मीडिया पोस्ट, वीडियो और ऑडियो रिकॉर्डिंग, सीसीटीवी फुटेज जैसे साक्ष्य महिला पीड़िताओं की आवाज़ को बल देते हैं और उनकी पीड़ा को न्यायालय में प्रमाणित करने का साधन बनते हैं। डिजिटल साक्ष्य का महत्व इस तथ्य में निहित है कि यह अपराध को

प्रत्यक्ष या परोक्ष रूप से सिद्ध करने में मदद करता है। यह पीड़िता की गवाही को मजबूती प्रदान करता है और आरोपी के अपराध की सच्चाई को उजागर करता है। इसके साथ ही, यह न्याय प्रणाली को तकनीकी युग के अनुरूप संवेदनशील और सशक्त बनाता है। हालाँकि, डिजिटल साक्ष्य के उपयोग में कई चुनौतियाँ भी हैं। सबसे बड़ी चुनौती इन साक्ष्यों की प्रमाणिकता और विश्वसनीयता बनाए रखने की होती है। तकनीक के माध्यम से साक्ष्यों को बदला या मिटाया जा सकता है, इसलिए इन्हें सुरक्षित रखना कठिन कार्य है। दूसरी चुनौती यह है कि कई बार डेटा देश की सीमाओं के बाहर संग्रहीत होता है, जिससे उसे समय पर प्राप्त करना मुश्किल हो जाता है। साथ ही, निजता और मानवाधिकार से जुड़े प्रश्न भी उठते हैं कि कहीं डिजिटल साक्ष्य एक व्यक्ति की स्वतंत्रता का उल्लंघन न कर दें। महिला पीड़िताओं के संदर्भ में यह समस्या और भी गंभीर है, क्योंकि अधिकांश मामलों में वे पहले से ही सामाजिक, आर्थिक और मानसिक दबाव का सामना कर रही होती हैं। न्याय पाने के लिए उन्हें न केवल अपराधी से लड़ना होता है, बल्कि तकनीकी और कानूनी जटिलताओं से भी जूझना पड़ता है। ऐसे में डिजिटल साक्ष्य उनके लिए न्याय की एक आशा और शक्ति का प्रतीक बनते हैं। यह शोधपत्र इस बात पर केंद्रित है कि डिजिटल - साक्ष्य महिलाओं के विरुद्ध साइबर अपराधों में किस प्रकार निर्णायक भूमिका निभाते हैं, उनकी उपयोगिता और सीमाएँ क्या हैं, और इनसे जुड़े व्यावहारिक व सामाजिक पहलू क्या हैं। साथ ही, यह अध्ययन यह भी स्पष्ट करता है कि डिजिटल साक्ष्य केवल अपराध को साबित करने का माध्यम नहीं, बल्कि पीड़िताओं के आत्मविश्वास को पुनर्स्थापित करने और समाज में न्याय की भावना को मजबूत करने का महत्वपूर्ण साधन भी है।

प्रस्तावना

21वीं सदी में इंटरनेट और डिजिटल प्रौद्योगिकी ने मानव जीवन को नई दिशा दी है। सामाजिक संपर्क, व्यापार, शिक्षा और मनोरंजन का बड़ा हिस्सा अब आभासी दुनिया) Virtual World) पर आधारित है। लेकिन तकनीक का

यह विस्तार अपराधियों के लिए भी नए अवसर लेकर आया है। इसी कारण **साइबर अपराध** आधुनिक युग की सबसे गंभीर चुनौतियों में से एक बन चुका है। महिलाएँ साइबर अपराध का सबसे संवेदनशील वर्ग मानी जाती हैं। ऑनलाइन स्टॉकिंग, फेक प्रोफाइल बनाना, मॉर्फिंग और डीपफेक्स, गैर-सहमति से निजी तस्वीरें या वीडियो साझा करना) Revenge Porn), साइबर बुलिंग और वित्तीय धोखाधड़ी जैसी घटनाएँ आज आम होती जा रही हैं। इन अपराधों से महिलाओं की निजता, गरिमा और सुरक्षा सीधे-सीधे प्रभावित होती है। इन अपराधों के निवारण और अभियोजन में **डिजिटल साक्ष्य) Digital Evidence)** की भूमिका निर्णायक है। इलेक्ट्रॉनिक मेल, चैट लॉग्स, सोशल मीडिया पोस्ट, मेटाडेटा, सीसीटीवी फुटेज, कॉल रिकॉर्डिंग, या क्लाउड सर्वर पर संग्रहीत डाटा – सब कुछ आज न्यायालय में प्रमाण के रूप में प्रस्तुत किया जा सकता है। परंतु यह तभी संभव है जब साक्ष्य को **विधिक रूप से मान्यता** प्राप्त हो और उसका संरक्षण सही तरीके से किया गया हो। भारत में अब **भारतीय साक्ष्य अधिनियम, 2023 (Bhartiya Sakshya Adhiniyam, 2023)** लागू हो चुका है, जिसने पुराने 1872 के अधिनियम को प्रतिस्थापित किया है। इस नए अधिनियम में इलेक्ट्रॉनिक अभिलेखों) Electronic Records) को परिभाषित कर उन्हें स्पष्ट रूप से **प्राथमिक साक्ष्य) Primary Evidence)** के रूप में स्वीकार किया गया है। इसी प्रकार **भारतीय न्याय संहिता, 2023 (BNS)** ने महिलाओं के विरुद्ध साइबर अपराधों को स्पष्ट रूप से परिभाषित किया है।

साइबर अपराध और महिला पीड़ित

डिजिटल युग में इंटरनेट और सोशल मीडिया ने महिलाओं को अपनी अभिव्यक्ति, शिक्षा, व्यापार और सामाजिक सहभागिता का अभूतपूर्व अवसर प्रदान किया है। किंतु इसके साथ ही आभासी दुनिया महिलाओं के लिए नए प्रकार की असुरक्षा और उत्पीड़न भी लेकर आई है। यदि परंपरागत अपराध महिलाओं के शरीर और भौतिक उपस्थिति पर केंद्रित थे, तो **साइबर अपराध उनकी निजता, गरिमा और डिजिटल पहचान पर हमला करते हैं।**

प्रमुख साइबर अपराध जिनसे महिलाएँ प्रभावित होती हैं

(A) साइबर स्टॉकिंग (Cyber Stalking)

- किसी महिला की ऑनलाइन गतिविधियों की लगातार निगरानी करना, उसे ई-मेल, चैट या सोशल मीडिया पर बार-बार संदेश भेजना या धमकी देना।
- BNS 2023 की धारा 78 (Stalking) में साइबर स्टॉकिंग को स्पष्ट रूप से अपराध माना गया है।
- उदाहरण: सोशल मीडिया पर किसी महिला का पीछा करना, लगातार लोकेशन ट्रैक करना।

(B) रिवेंज पोर्न और गैर-सहमति से निजी सामग्री का प्रसार

- प्रेम संबंध टूटने के बाद या ब्लैकमेल करने के उद्देश्य से महिला की निजी तस्वीरें/वीडियो इंटरनेट पर प्रसारित करना।
- IT Act, 2000 की धारा 67, 67A और BNS 2023 की धारा 77 (Voyeurism) लागू होती हैं।
- यह अपराध पीड़िता को दोहरी यातना देता है – सामाजिक बदनामी और न्यायिक प्रक्रिया में पुनः उत्पीड़न।

(C) मॉर्फिंग और डीपफेक (Morphing and Deepfakes)

- किसी महिला की तस्वीर को एडिट कर अश्लील सामग्री में प्रयोग करना या डीपफेक तकनीक से उसकी नकली वीडियो बनाना।
- यह न केवल निजता का उल्लंघन है बल्कि तकनीकी रूप से इसे रोकना भी चुनौतीपूर्ण है।
- BNS 2023 की **धारा 294 (Obscenity)** और IT Act के प्रावधान लागू होते हैं।

(D) साइबर बुलिंग और ट्रोलिंग

- सोशल मीडिया पर अपमानजनक टिप्पणियाँ, धमकी भरे संदेश या ट्रोलिंग।
- कई बार संगठित" ऑनलाइन गैंग "महिलाओं, खासकर पत्रकारों, एक्टिविस्टों और नेताओं को निशाना बनाते हैं।
- इससे अभिव्यक्ति की स्वतंत्रता भी प्रभावित होती है।

(E) फेक प्रोफाइल और पहचान चोरी (Identity Theft)

- किसी महिला की नकली प्रोफाइल बनाकर धोखाधड़ी करना, अश्लील सामग्री डालना या दूसरों को गुमराह करना।
- IT Act की **धारा 66C (Identity Theft)** और **66D (Cheating by Personation)** यहाँ लागू होती हैं।

(F) वित्तीय साइबर अपराध (Financial Frauds)

- फिशिंग ई-मेल, ऑनलाइन लोन ऐप्स के जरिए महिलाओं को ठगना।
- कई मामलों में निजी फोटो या डेटा को" डेटा लीक "की धमकी देकर ब्लैकमेल किया जाता है।

3. प्रभाव (Impact on Women Victims)

1. **मनोवैज्ञानिक प्रभाव:**
    - अवसाद, चिंता, आत्मसम्मान की हानि।
    - कई मामलों में आत्महत्या तक की प्रवृत्ति।
2. **सामाजिक प्रभाव:**
    - परिवार और समाज से समर्थन न मिलना।
    - पीड़िता को ही दोषी ठहराया जाना) Victim Blaming)।
3. **कानूनी व न्यायिक प्रभाव:**
    - पीड़िता को पुलिस थाने में शिकायत दर्ज कराने में कठिनाई।
    - डिजिटल साक्ष्य को सही ढंग से एकत्र और सुरक्षित न रख पाने की समस्या।

डिजिटल साक्ष्य का महत्व

डिजिटल साक्ष्य आज के युग में अपराध की जाँच और अभियोजन की रीढ़ बन चुका है। पारंपरिक अपराधों की तरह साइबर अपराधों में भौतिक साक्ष्य) physical evidence) मिलना कठिन होता है, इसलिए इलेक्ट्रॉनिक डाटा ही सच्चाई का सबसे बड़ा प्रमाण माना जाता है। महिला पीड़ितों से संबंधित साइबर अपराधों – जैसे **ऑनलाइन उत्पीड़न, अश्लील संदेश भेजना, मॉर्फ्ड तस्वीरें बनाना, साइबर स्टॉकिंग, फेक प्रोफाइल तैयार करना, बदनामी करना** आदि – को सिद्ध करने के लिए डिजिटल साक्ष्य सबसे प्रमुख साधन हैं।

ईमेल, सोशल मीडिया चैट, व्हाट्सएप मैसेज, सीसीटीवी फुटेज, मोबाइल रिकॉर्डिंग, कॉल डिटेल्स, इंटरनेट लॉग्स और कंप्यूटर/मोबाइल से प्राप्त फॉरेंसिक डाटा अदालत में महिला पीड़िता की बात को साबित करने में मदद करते हैं। **भारतीय साक्ष्य अधिनियम, 2023 की धारा 57 और 61** ने इलेक्ट्रॉनिक रिकॉर्ड को विधिक मान्यता दी है, जिससे अब डिजिटल साक्ष्य को भौतिक साक्ष्य के समान ही स्वीकार किया जाता है। यह महिलाओं को न्याय दिलाने और अपराधियों को दंडित करने का मजबूत माध्यम है।

डिजिटल साक्ष्य का कानूनी ढांचा

साइबर अपराध के मामलों में दोषसिद्धि और न्याय सुनिश्चित करने के लिए **डिजिटल साक्ष्य) Digital Evidence)** की भूमिका अत्यंत महत्वपूर्ण है। परंतु केवल तकनीकी साक्ष्य पर्याप्त नहीं होता; उसे विधिक रूप से **ग्राह्य) Admissible)** और **विश्वसनीय) Reliable)** भी होना चाहिए। इसी कारण डिजिटल साक्ष्य का विधिक ढांचा भारतीय और अंतरराष्ट्रीय स्तर पर लगातार विकसित हो रहा है।

अंतरराष्ट्रीय विधिक ढांचा

(A) बुडापेस्ट कन्वेंशन ऑन साइबरक्राइम (2001)

- यह पहला और सबसे महत्वपूर्ण अंतरराष्ट्रीय समझौता है जिसने इलेक्ट्रॉनिक साक्ष्य के लिए मानक निर्धारित किए।
- इसमें डेटा संरक्षण, लॉग्स को सुरक्षित रखने, और अंतरराष्ट्रीय सहयोग से डिजिटल साक्ष्य साझा करने की प्रक्रिया तय की गई।
- भारत अभी इसका हस्ताक्षरकर्ता नहीं है, परंतु इसकी अनुशंसाएँ भारतीय न्यायिक विमर्श को प्रभावित करती हैं।

(B) UN Resolution on Online Violence Against Women (2015)

- संयुक्त राष्ट्र महासभा ने महिला पीड़ितों के विरुद्ध ऑनलाइन हिंसा को गंभीर अपराध माना।
- इसमें राज्यों को यह निर्देश दिया गया कि वे डिजिटल साक्ष्य के संरक्षण और प्रस्तुति हेतु मजबूत विधिक ढाँचा तैयार करें।

(C) यूरोपीय संघ (EU) का GDPR और e-Evidence Package

- GDPR निजता और डेटा सुरक्षा पर बल देता है।
- e-Evidence नियमों के तहत सदस्य देशों की अदालतें दूसरे देशों से डिजिटल साक्ष्य की मांग कर सकती हैं।

भारत में विधिक ढांचा

भारत में साइबर अपराध और डिजिटल साक्ष्य को नियंत्रित करने के लिए तीन प्रमुख विधिक स्तंभ हैं –

1. **सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000)**

2. **भारतीय न्याय संहिता, 2023 (BNS, 2023)**

3. **भारतीय साक्ष्य अधिनियम, 2023 (Bhartiya Sakshya Adhiniyam, 2023)**

सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000)

भारत में **ई-कॉमर्स और इंटरनेट उपयोग** की तेज़ी से बढ़ती प्रवृत्ति को देखते हुए सूचना प्रौद्योगिकी अधिनियम, 2000 लागू किया गया। इसका मुख्य उद्देश्य था: इलेक्ट्रॉनिक रिकॉर्ड्स और डिजिटल सिग्नेचर को कानूनी मान्यता देना; साइबर अपराधों को परिभाषित करना और उनके लिए दंड निर्धारित करना; ई-गवर्नेंस और ऑनलाइन लेन-देन को वैध बनाना। यह अधिनियम **17 अक्तूबर 2000** से लागू हुआ।

अधिनियम की प्रमुख विशेषताएँ

(i) **इलेक्ट्रॉनिक रिकॉर्ड्स और डिजिटल सिग्नेचर को वैधता**: IT Act ने ईमेल, ऑनलाइन डॉक्यूमेंट, डिजिटल सिग्नेचर आदि को "कानूनी साक्ष्य" का दर्जा दिया।

(ii) **साइबर अपराधों का निर्धारण और दंड**: हैकिंग, डाटा चोरी, अश्लील सामग्री का प्रकाशन, साइबर स्टॉकिंग आदि अपराधों के लिए सज़ा और जुर्माना तय किया गया।

(iii)**CERT-In (Computer Emergency Response Team-India)**: 2008 संशोधन के बाद CERT-In को राष्ट्रीय नोडल एजेंसी बनाया गया ताकि साइबर सुरक्षा घटनाओं पर तुरंत कार्यवाही हो।

(iv)**न्यायाधिकरण और विशेष अदालतें**: साइबर अपराधों के मामलों के लिए *Adjudicating Officers* और *Cyber Appellate Tribunal* का प्रावधान किया गया।

महिलाओं से जुड़े अपराध और IT Act की धाराएँ

महिला पीड़िताओं के खिलाफ ऑनलाइन अपराधों को रोकने में IT Act की विशेष भूमिका है। कुछ महत्वपूर्ण धाराएँ:

(A) धारा 66 (**कंप्यूटर संबंधी अपराध**): इसमें *हैकिंग, अनधिकृत प्रवेश, डेटा की चोरी* शामिल हैं। महिला के सोशल मीडिया अकाउंट को हैक कर आपत्तिजनक सामग्री डालना धारा 66 के अंतर्गत अपराध है।

(B) धारा 66C (**पहचान की चोरी**): किसी महिला की पहचान, फोटो या दस्तावेज़ का दुरुपयोग करना। उदाहरण: महिला के नाम से फर्जी फेसबुक/इंस्टाग्राम प्रोफाइल बनाना।

(C) धारा 66D (**धोखाधड़ी**): ऑनलाइन धोखाधड़ी या महिला को फर्जी आईडी से ब्लैकमेल करना।

(D) धारा 66E (**निजता का उल्लंघन**): किसी महिला की सहमति बिना उसकी निजी तस्वीर खींचना, रिकॉर्ड करना या साझा करना। दंड: 3 वर्ष तक की कैद या ₹2 लाख तक जुर्माना।

(E) धारा 67 (**अश्लील सामग्री का प्रकाशन**): अश्लील सामग्री (Pornography) को प्रकाशित/प्रेषित करना। महिला की आपत्तिजनक फोटो/वीडियो इंटरनेट पर डालना इस धारा के तहत आता है।

(F) धारा 67A (**यौन रूप से स्पष्ट सामग्री**): यदि सामग्री "Sexually Explicit" है, तो दंड और भी कठोर है (5 वर्ष कैद + जुर्माना)।

(G) धारा 67B (**यौन रूप से स्पष्ट सामग्री**): 18 वर्ष से कम आयु की लड़कियों की अश्लील सामग्री बनाना, डाउनलोड करना या साझा करना। यह POCSO Act के साथ-साथ लागू होती है।

भारतीय न्याय संहिता, 2023 (BNS, 2023) – महिलाओं और साइबर अपराध के संदर्भ में

भारतीय न्याय संहिता, 2023 (BNS) ने भारतीय दंड संहिता, 1860 का स्थान ले लिया है और इसे 1 जुलाई 2024 से लागू किया गया। इसका उद्देश्य अपराधों को आधुनिक स्वरूप प्रदान करना और डिजिटल युग में बढ़ते साइबर अपराधों को विधिक ढाँचे में सम्मिलित करना है। पारंपरिक अपराधों के साथ-साथ इसमें महिला पीड़ितों के विरुद्ध साइबर अपराधों को विशेष रूप से परिभाषित किया गया है।

महिलाओं से संबंधित अपराधों के संदर्भ में BNS ने कई महत्वपूर्ण धाराओं को शामिल किया है। उदाहरण के लिए, धारा 340(2) साइबर धोखाधड़ी को परिभाषित करती है, जहाँ कोई व्यक्ति डिजिटल माध्यम से नकली पहचान बनाकर किसी महिला को धोखा देता है या उसका शोषण करता है। इसी प्रकार, धारा 319, 338, 336 पहचान की चोरी) Identity Theft) को अपराध मानती है, जिसके अंतर्गत महिला की व्यक्तिगत जानकारी, पासवर्ड या फोटो का अवैध प्रयोग आता है। धारा 77 साइबर स्टॉकिंग को परिभाषित करती है, जिसमें बार-बार ऑनलाइन पीछा करना, संदेश भेजना, या नकली प्रोफ़ाइल बनाना शामिल है। यह विशेष रूप से महिलाओं के लिए एक गंभीर समस्या है और इस धारा के तहत पहली बार अपराध करने पर तीन वर्ष तक की सजा तथा पुनरावृत्ति पर पाँच वर्ष तक की सजा का प्रावधान है।

महिलाओं की गरिमा और निजता की सुरक्षा के लिए भी BNS में विशेष प्रावधान किए गए हैं। धारा 75 यौन उत्पीड़न को परिभाषित करती है, जिसमें अश्लील संदेश, ईमेल, चित्र या सोशल मीडिया पोस्ट भेजना आता है। धारा 78 पीछा करने) Stalking) से संबंधित है और इसमें डिजिटल स्टॉकिंग को भी सम्मिलित किया गया है। धारा 77 में

निजता के उल्लंघन) Voyeurism) को अपराध माना गया है, जिसमें किसी महिला की अनुमति के बिना उसकी तस्वीर या वीडियो लेना अथवा साझा करना दंडनीय है। इसके अतिरिक्त धारा 79 यौन शोषण और आपत्तिजनक चित्रण से संबंधित है, जहाँ महिला की मॉर्फ की गई तस्वीरें या वीडियो बनाना और फैलाना अपराध की श्रेणी में आता है।

साइबर अश्लीलता और पोर्नोग्राफी को भी BNS ने अपराध घोषित किया है। धारा के अंतर्गत अश्लील सामग्री का इलेक्ट्रॉनिक माध्यम से प्रकाशन अपराध है, जबकि धारा 294 बच्चों से संबंधित अश्लील सामग्री) Child Pornography) को परिभाषित करती है, जिसमें नाबालिग लड़कियों की तस्वीरें अथवा वीडियो सम्मिलित करना कठोर दंडनीय अपराध है।

इस प्रकार, भारतीय न्याय संहिता, 2023 महिलाओं के प्रति साइबर अपराधों को रोकने और दंडित करने के लिए एक आधुनिक और सशक्त कानूनी ढाँचा प्रस्तुत करती है। यह कानून महिलाओं को पहचान की चोरी, साइबर स्टॉकिंग, डिजिटल अश्लीलता, और ऑनलाइन उत्पीड़न जैसे नए स्वरूप के अपराधों से सुरक्षा प्रदान करता है। IT Act, 2000 और भारतीय साक्ष्य अधिनियम, 2023 के साथ मिलकर यह एक त्रिकोणीय कानूनी तंत्र बनाता है, जो साइबर अपराधों की रोकथाम और न्याय सुनिश्चित करने में अत्यंत प्रभावी है।

भारतीय साक्ष्य अधिनियम, 2023 (BSA, 2023) और डिजिटल साक्ष्य का महत्व

भारतीय साक्ष्य अधिनियम, 2023 (BSA) ने पुराने भारतीय साक्ष्य अधिनियम, 1872 को प्रतिस्थापित कर दिया है और इसे डिजिटल युग के अनुरूप बनाया गया है। आज के समय में अपराधों का स्वरूप काफी हद तक ऑनलाइन माध्यम से जुड़ गया है, इसलिए अदालतों में प्रस्तुत किए जाने वाले साक्ष्यों में डिजिटल साक्ष्य का महत्व अत्यधिक बढ़ गया है। BSA, 2023 ने इलेक्ट्रॉनिक और डिजिटल रिकॉर्ड्स को स्पष्ट रूप से साक्ष्य की श्रेणी में मान्यता दी है।

नए अधिनियम की धारा 57 और धारा 61 विशेष रूप से महत्वपूर्ण हैं। धारा 57 इलेक्ट्रॉनिक अभिलेखों) Electronic Records) को प्राथमिक साक्ष्य के रूप में स्वीकार करती है। इसका अर्थ यह है कि ईमेल, व्हाट्सएप चैट, सोशल मीडिया पोस्ट, कॉल रिकॉर्डिंग, सीसीटीवी फुटेज, कंप्यूटर फाइलें, सर्वर लॉग्स और ब्लॉकचेन रिकॉर्ड्स को अदालत में वैध साक्ष्य माना जाएगा। वहीं धारा 61 इलेक्ट्रॉनिक अभिलेखों की प्रमाणिकता और सत्यापन के लिए डिजिटल हस्ताक्षर और सुरक्षित इलेक्ट्रॉनिक प्रमाणपत्र की व्यवस्था करती है।

महिला पीड़ितों से संबंधित साइबर अपराधों में यह प्रावधान और भी महत्त्वपूर्ण हो जाता है। उदाहरण के लिए, यदि किसी महिला को साइबर स्टॉकिंग, मॉर्फ्ड इमेजेस, या अश्लील सामग्री के प्रसार का सामना करना पड़े, तो उसकी सोशल मीडिया चैट, ईमेल, और मोबाइल डेटा अदालत में सीधे प्रमाण के रूप में प्रस्तुत किए जा सकते हैं। पहले यह

आवश्यक था कि इलेक्ट्रॉनिक साक्ष्य को धारा 65B (पुराने अधिनियम (के तहत प्रमाणित किया जाए, लेकिन अब BSA, 2023 ने इस प्रक्रिया को सरल बनाकर डिजिटल साक्ष्यों की स्वीकार्यता को और भी व्यावहारिक और पीड़िता-हितैषी बना दिया है।

इसके अतिरिक्त, धारा 58 और धारा 60 डिजिटल साक्ष्यों की द्वितीयक प्रतियों) Secondary Evidence) के उपयोग को भी अनुमति देती हैं। उदाहरण के लिए, यदि मूल सर्वर तक पहुँच संभव न हो, तो हार्ड ड्राइव की क्लोन कॉपी या क्लाउड से डाउनलोड की गई कॉपी भी अदालत में स्वीकार्य होगी। यह विशेष रूप से तब महत्वपूर्ण है जब महिला पीड़ित विदेश-आधारित सोशल मीडिया प्लेटफ़ॉर्म) जैसे मेटा, इंस्टाग्राम, या ट्विटर (पर उत्पीड़न का सामना करती है और मूल सर्वर तक पहुँचना कठिन होता है।

BSA, 2023 ने डिजिटल फॉरेंसिक और प्रमाणिकता की भी नई राह खोली है। इसमें इलेक्ट्रॉनिक साक्ष्यों को सुरक्षित रखने के लिए **चेन ऑफ कस्टडी) Chain of Custody)** के सिद्धांत को मान्यता दी गई है। यानी किसी भी डिजिटल साक्ष्य को जब्त करने से लेकर अदालत में प्रस्तुत करने तक उसकी निरंतरता और विश्वसनीयता सुनिश्चित करना आवश्यक होगा।

संक्षेप में कहा जाए तो भारतीय साक्ष्य अधिनियम, 2023 ने डिजिटल साक्ष्यों को न केवल मान्यता दी है, बल्कि उन्हें अपराध साबित करने का एक सशक्त साधन बना दिया है। विशेषकर साइबर अपराधों की शिकार महिलाओं के लिए यह अधिनियम न्याय प्राप्ति की राह को सरल बनाता है, क्योंकि अब उनकी डिजिटल बातचीत, फोटो, वीडियो, और तकनीकी रिकॉर्ड अदालत में सीधे और प्रभावी रूप से स्वीकार किए जा सकते हैं। इस प्रकार यह अधिनियम IT Act, 2000 और BNS, 2023 के साथ मिलकर महिलाओं के खिलाफ साइबर अपराधों से निपटने का ठोस आधार प्रदान करता है।

प्रामाणिक न्यायिक निर्णय

1. स्टेट ऑफ़ तमिलनाडु बनाम सुहास कट्टी

यह भारत का पहला महत्त्वपूर्ण मामला था जिसमें एक महिला के विरुद्ध अश्लील संदेश और मॉर्फ्ड तस्वीरें इंटरनेट पर डाली गईं। अदालत ने आरोपी को **सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 67** तथा भारतीय दंड संहिता की धारा 509 के अंतर्गत दोषी ठहराया। इस मामले में ईमेल और चैट रिकॉर्ड को **डिजिटल साक्ष्य** के रूप में स्वीकार किया गया। यह निर्णय इस बात का प्रमाण है कि महिलाओं के खिलाफ साइबर उत्पीड़न को न्यायालय गंभीर अपराध मानता है और डिजिटल साक्ष्य उनकी सुरक्षा सुनिश्चित करने का मुख्य साधन है।

2. श्रेय सिंघल बनाम भारत संघ (2015)

इस मामले में सर्वोच्च न्यायालय ने सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 66A को असंवैधानिक घोषित किया क्योंकि यह अभिव्यक्ति की स्वतंत्रता) अनुच्छेद 19(1)(a)) पर अनुचित प्रतिबंध लगाती थी। यद्यपि इस धारा का उपयोग महिलाओं के ऑनलाइन उत्पीड़न को रोकने के लिए भी किया जाता था, लेकिन इसके दुरुपयोग के कारण इसे रद्द कर दिया गया। यह फैसला महत्वपूर्ण है क्योंकि इसके बाद महिलाओं से संबंधित साइबर अपराधों के निपटारे के लिए अब **भारतीय न्याय संहिता, 2023 की धाराएँ** उपयोग में लाई जाती हैं।

3. धरमबीर बनाम सीबीआई (2008)

इस मामले में प्रश्न यह था कि क्या सीडी और अन्य इलेक्ट्रॉनिक रिकॉर्ड अदालत में साक्ष्य के रूप में स्वीकार्य हैं। दिल्ली उच्च न्यायालय ने स्पष्ट किया कि डिजिटल साक्ष्य तभी स्वीकार्य होंगे जब उन्हें **भारतीय साक्ष्य अधिनियम, 1872 की धारा 65B** के अनुरूप प्रमाणित किया जाए। अब यही प्रावधान **भारतीय साक्ष्य अधिनियम, 2023 (Bharatiya Sakshya Adhiniyam, 2023) की धारा 57 और 61** में शामिल है। यह फैसला महिलाओं से संबंधित साइबर अपराधों में महत्त्वपूर्ण है क्योंकि चैट, व्हाट्सएप संदेश, ईमेल और वीडियो जैसे साक्ष्य तभी मान्य होंगे जब उनकी सत्यता विधिक प्रक्रिया द्वारा प्रमाणित हो।

4. अर्जुन पांडित्राव खोतकर बनाम कैलाश कुशनराव गोरंट्याल (2020)

इस मामले में सर्वोच्च न्यायालय ने यह कहा कि यदि डिजिटल साक्ष्य प्रस्तुत किए जाते हैं तो उनके साथ **65B प्रमाणपत्र** अनिवार्य होना चाहिए। यह निर्णय महिलाओं से जुड़े साइबर अपराधों) जैसे अश्लील वीडियो, सोशल मीडिया चैट रिकॉर्ड (के संदर्भ में महत्वपूर्ण है क्योंकि अब अदालतें डिजिटल साक्ष्य तभी स्वीकार करती हैं जब उनकी प्रामाणिकता उचित तरीके से सिद्ध की गई हो।

5. मनोजहर लाल शर्मा बनाम भारत संघ (पेगासस केस, 2021)

इस मामले में आरोप था कि पेगासस नामक स्पाइवेयर के माध्यम से कई महिलाओं और पत्रकारों की जासूसी की गई। सर्वोच्च न्यायालय ने निजता के अधिकार) अनुच्छेद 21) को ध्यान में रखते हुए एक स्वतंत्र तकनीकी समिति गठित की। इस फैसले ने यह सिद्ध किया कि महिलाओं की डिजिटल सुरक्षा और निजता उनके जीवन और स्वतंत्रता का अभिन्न हिस्सा है।

6. खुर्शीद अहमद खान बनाम उत्तर प्रदेश राज्य (2015)

इस मामले में सर्वोच्च न्यायालय ने महिलाओं की गरिमा और सम्मान को सर्वोपरि माना तथा कहा कि किसी भी प्रकार का आचरण जो महिला की गरिमा को ठेस पहुँचाता है, वह संविधान के अनुच्छेद 21 (जीवन और स्वतंत्रता का अधिकार (का उल्लंघन है। साइबर अपराधों के संदर्भ में यह निर्णय महत्वपूर्ण है क्योंकि ऑनलाइन उत्पीड़न और मॉर्फ्ड इमेज जैसी गतिविधियाँ सीधे तौर पर महिला की गरिमा को प्रभावित करती हैं।

7. अनवर पी.वी. बनाम पी.के. बशीर (2014)

इस मामले में सर्वोच्च न्यायालय ने कहा कि इलेक्ट्रॉनिक साक्ष्य को तभी स्वीकार किया जाएगा जब उनके साथ धारा 65B का प्रमाणपत्र प्रस्तुत किया जाए। यह निर्णय डिजिटल साक्ष्यों की स्वीकार्यता का आधारभूत स्तंभ माना जाता है और महिलाओं से जुड़े साइबर अपराधों के मामलों में भी अत्यंत प्रासंगिक है।

डिजिटल साक्ष्य की चुनौतियाँ

हालाँकि, डिजिटल साक्ष्य की स्वीकार्यता और विश्वसनीयता को लेकर कई चुनौतियाँ भी सामने आती हैं। सबसे बड़ी चुनौती **प्रमाणिकता) authenticity) और अखंडता) integrity)** की है। डिजिटल डाटा आसानी से बदला या मिटाया जा सकता है, इसलिए अदालत में यह साबित करना आवश्यक होता है कि प्रस्तुत किया गया साक्ष्य छेड़छाड़ से मुक्त है। इसके लिए **65B प्रमाणपत्र** (अब भारतीय साक्ष्य अधिनियम 2023 की धारा 63) अनिवार्य कर दिया गया है, परंतु व्यावहारिक रूप से पुलिस और वकीलों को इसकी प्रक्रिया समझने में कठिनाई होती है।

दूसरी चुनौती है **तकनीकी जटिलता) technical complexity)।** कई बार अपराधी VPN, प्रॉक्सी सर्वर, डार्क वेब या एनक्रिप्शन का प्रयोग करते हैं, जिससे अपराध का स्रोत ढूँढना मुश्किल हो जाता है। महिला पीड़िताएँ अक्सर सोशल मीडिया प्लेटफॉर्म से जुड़े मामलों में न्याय पाने के लिए संघर्ष करती हैं क्योंकि कई बार कंपनियाँ भारत के अधिकार क्षेत्र में नहीं आतीं और डाटा उपलब्ध कराने में देरी करती हैं।

इसके अतिरिक्त **गोपनीयता) privacy) और निजता) right to privacy)** से जुड़ी दिक्कतें भी सामने आती हैं। डिजिटल साक्ष्य जुटाते समय यह सुनिश्चित करना आवश्यक है कि पीड़िता की निजता का उल्लंघन न हो। उदाहरण के लिए, यदि किसी महिला की आपत्तिजनक तस्वीरें अदालत में साक्ष्य के रूप में प्रस्तुत की जाती हैं तो यह उसके सम्मान और मानसिक स्थिति पर विपरीत असर डाल सकता है।

अंततः, **न्यायपालिका और पुलिस बल में तकनीकी विशेषज्ञता की कमी** भी एक गंभीर समस्या है। डिजिटल साक्ष्यों का उचित तरीके से संग्रह, संरक्षण और विश्लेषण करने के लिए विशेष प्रशिक्षण और आधुनिक फॉरेंसिक लैब की आवश्यकता होती है।

निष्कर्ष (Conclusion)

साइबर अपराधों के बढ़ते स्वरूप ने यह स्पष्ट कर दिया है कि डिजिटल साक्ष्य आज न्यायिक प्रणाली में अत्यंत महत्वपूर्ण भूमिका निभाते हैं। विशेष रूप से महिला पीड़ितों से संबंधित अपराधों – जैसे साइबर स्टॉकिंग, ऑनलाइन उत्पीड़न, फेक प्रोफाइल बनाना, और अश्लील सामग्री का प्रसार – में पारंपरिक साक्ष्य अक्सर अनुपलब्ध होते हैं। ऐसे में इलेक्ट्रॉनिक रिकॉर्ड ही अपराध की सच्चाई को उजागर करने का सबसे प्रभावी साधन बनता है।

भारतीय न्याय संहिता, 2023 तथा भारतीय साक्ष्य अधिनियम, 2023 ने डिजिटल साक्ष्यों को विधिक मान्यता प्रदान करके एक सकारात्मक कदम उठाया है। इसके बावजूद, न्यायिक प्रक्रिया में अनेक चुनौतियाँ बनी हुई हैं – जैसे साक्ष्यों की प्रामाणिकता सिद्ध करना, तकनीकी जटिलताओं से निपटना, पीड़िता की निजता की रक्षा करना और सीमा-पार डाटा प्राप्ति में आने वाली बाधाएँ। इन चुनौतियों को दूर किए बिना महिला पीड़िताओं को पूर्ण न्याय दिलाना कठिन रहेगा।

अतः, डिजिटल साक्ष्य को न्याय की प्रक्रिया में अधिक प्रभावी बनाने के लिए कानून, तकनीक और सामाजिक दृष्टिकोण – तीनों स्तरों पर समन्वित सुधार की आवश्यकता है।

नीतिगत सुधार और सुझाव (Policy Reforms & Suggestions)

1. **विशेष प्रशिक्षण एवं अवसंरचना** – पुलिस, अभियोजन पक्ष और न्यायपालिका को डिजिटल साक्ष्य से संबंधित विशेष प्रशिक्षण दिया जाना चाहिए। हर राज्य में आधुनिक साइबर फॉरेंसिक प्रयोगशालाएँ स्थापित की जानी चाहिए।

2. **स्पष्ट विधिक प्रावधान** – भारतीय साक्ष्य अधिनियम, 2023 में डिजिटल साक्ष्य की स्वीकृति की प्रक्रिया को और सरल और स्पष्ट बनाया जाए ताकि महिला पीड़िताओं के मामलों में अनावश्यक तकनीकी बाधाएँ न आएँ।

3. **गोपनीयता और संरक्षण** – महिला पीड़िताओं की निजता बनाए रखने के लिए 'इन-कैमरा ट्रायल' और संवेदनशील साक्ष्यों के प्रकाशन पर प्रतिबंध जैसे प्रावधानों का कड़ाई से पालन होना चाहिए।

4. **सीमा-पार सहयोग** – सोशल मीडिया और क्लाउड स्टोरेज कंपनियाँ अक्सर विदेशी न्यायक्षेत्र में आती हैं, इसलिए भारत को अंतरराष्ट्रीय समझौतों) जैसे **Budapest Convention**) में सक्रिय भागीदारी करनी चाहिए जिससे डिजिटल डाटा समय पर प्राप्त हो सके।

5. **तेज़ न्याय प्रक्रिया** – महिला पीड़िताओं से जुड़े साइबर अपराधों के लिए विशेष त्वरित न्यायालय) fast-track courts) स्थापित किए जाएँ, जो डिजिटल साक्ष्यों का मूल्यांकन तेजी से कर सकें।

6. **जन-जागरूकता अभियान** – महिलाओं और लड़कियों को डिजिटल सुरक्षा, ऑनलाइन धोखाधड़ी और साइबर उत्पीड़न से बचने के लिए जागरूक करना अत्यंत आवश्यक है। इसके लिए सरकार, शिक्षण संस्थान और सोशल मीडिया कंपनियाँ मिलकर कार्य करें।

7. **तकनीकी नवाचार** – ब्लॉकचेन जैसी तकनीक का उपयोग डिजिटल साक्ष्य की **chain of custody** सुरक्षित रखने के लिए किया जा सकता है, जिससे अदालत में उसकी विश्वसनीयता और बढ़ सके।

संदर्भ सूची

विधि (Statutes)

- भारतीय साक्ष्य अधिनियम, 2023।
- सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act, 2000)।
- भारतीय दंड संहिता) Bharatiya Nyaya Sanhita), 2023।
- जनरल डेटा प्रोटेक्शन रेगुलेशन) GDPR), 2016 (यूरोपीय संघ(।

पुस्तकें (Books)

- एन.एस .गोपालकृष्णन और टी.जी .अग्रवाल, *सूचना प्रौद्योगिकी कानून और साइबर अपराध* (Eastern Book Company 2019)।
- एस .रवि शंकर, *साइबर लॉ : इंटरनेट रेगुलेशन एंड साइबर क्राइम्स* (Taxmann Publications 2020)।
- **नमिता मल्होत्रा,** *साइबर न्यायशास्त्र की ओर : भारत में कानून, लैंगिकता और प्रौद्योगिकी* **(सेंटर फॉर इंटरनेट एंड सोसाइटी 2016)।**
- पी.के .सक्सेना, *इलेक्ट्रॉनिक एविडेंस एंड साइबर लॉ इन इंडिया* (LexisNexis 2021)।
- वी .कामाक्षी और ए .श्रीनिवास, साइबर क्राइम एंड डिजिटल एविडेंस लॉ) Universal Law Publishing 2018)।

- अपार गुप्ता, *भारतीय न्याय संहिता, 2023 पर टिप्पणियाँ* (ईबीसी पब्लिशिंग 2024)।
- एस.के .वर्मा, सूचना प्रौद्योगिकी और साइबर अपराध) Central Law Agency 2017)।
- वाकुल शर्मा, *सूचना प्रौद्योगिकी विधि और व्यवहार* (यूनिवर्सल लॉ पब्लिशिंग, 2021)।
- सुसन डब्ल्यू .ब्रेनर, *साइबर अपराध : साइबरस्पेस से आपराधिक खतरें* (प्रेगर सिक्योरिटी इंटरनेशनल 2010)।
- पवन दुग्गल, *साइबर क़ानून : भारतीय परिप्रेक्ष्य* (यूनिवर्सल लॉ पब्लिशिंग, 2019)।
- टाल ज़ास्र्की, *साइबर कानून और डिजिटल युग में मानवाधिकार* (कैम्ब्रिज यूनिवर्सिटी प्रेस 2020)।

शोध लेख (Articles)

- आर .जयशंकर, 'भारत में साइबर अपराध और महिला पीड़िताओं पर प्रभाव' (2021) 63(2) *Journal of Indian Law and Society* 145।
- सीमा चौधरी, 'डिजिटल साक्ष्य और भारतीय न्यायपालिका' (2022) 14 *National Law School Journal* 212।
- अनीता तिवारी, 'ऑनलाइन जेंडर आधारित हिंसा और कानून' (2023) 11(1) *Indian Journal of Gender Studies* 67।

ऑनलाइन स्रोत (Online Sources)

- इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार, 'CERT-In Notifications and Guidelines' (MeitY 2023) https://www.cert-in.org.in अभिगम 20 अगस्त 2025।
- सुप्रीम कोर्ट ऑफ इंडिया, 'Judgments Portal' (SCI 2025) https://www.sci.gov.in अभिगम 20 अगस्त 2025।
- यूरोपीय संघ, 'General Data Protection Regulation (GDPR) Portal' (EU 2024) https://gdpr-info.eu अभिगम 20 अगस्त 2025।