

डिजिटल स्पेस में महिलाओं के अधिकारों की रक्षा में भारतीय न्यायपालिका की भूमिका

¹ नेहा सक्सेना *

शोध छात्रा, विधि संकाय,
मदरहुड विश्वविद्यालय, रुड़की, उत्तराखण्ड

² डॉ. नलनीश चन्द्र सिंह

सह-आचार्य, विधि संकाय, मदरहुड विश्वविद्यालय, रुड़की, उत्तराखण्ड

सारांश

प्रौद्योगिकी की तीव्र प्रगति और डिजिटल स्पेस के विस्तार ने मानवीय संपर्क, सामाजिक भागीदारी और सूचना तक पहुँच के परिदृश्य को महत्वपूर्ण रूप से बदल दिया है। जहाँ इन क्रांतियों ने महिलाओं को सशक्तीकरण और आत्म-अभिव्यक्ति के अभूतपूर्व अवसर प्रदान किए हैं, वहीं उन्होंने उन्हें गोपनीयता, सुरक्षा और स्वतंत्रता से संबंधित अनूठे जोखिमों से भी अवगत कराया है। डिजिटल क्षेत्र में महिलाओं के सामने आने वाली उभरती चुनौतियों का पता लगाता है और उनके अधिकारों की रक्षा के लिए आवश्यक उपायों की विस्तृत जाँच प्रस्तुत करता है। विशेष रूप से, यह गोपनीयता, सुरक्षा और स्वतंत्रता के तीन महत्वपूर्ण क्षेत्रों पर ध्यान केंद्रित करता है। साइबर स्टॉकिंग, ऑनलाइन उत्पीड़न, डेटा गोपनीयता उल्लंघन और डिजिटल निगरानी जैसे मौजूदा खतरों की समीक्षा करके, चिंताओं को दूर करने में सक्रिय विधि, मजबूत डिजिटल साक्षरता कार्यक्रमों और वकालत समूहों की भूमिका के महत्व पर जोर देता है। अंततः, डिजिटल स्पेस में महिलाओं के अधिकारों की सुरक्षा कैसे की जा सकती है, तथा न्यायपालिका की भूमिका को भी दर्शाता है।

कीवर्ड: महिला सुरक्षा, डिजिटल युग, साइबर सुरक्षा, महिलाओं की गोपनीयता और स्वतंत्रता.

प्रस्तावना

भारत में, न्यायिक प्रणाली न्याय प्रशासन पर निगरानी रखने का काम करती है और महिलाओं के खिलाफ किए जाने वाले साइबर अपराधों की संख्या को कम करने में महत्वपूर्ण भूमिका निभाती है। यह कानूनी उपाय प्रदान करने, मिसाल कायम करने और यह सुनिश्चित करने के माध्यम से पूरा किया जाता है कि कानूनों को कुशल तरीके से लागू किया जाए। महिलाओं के खिलाफ ऑनलाइन हिंसा से निपटने के लिए, सुप्रीम कोर्ट संवैधानिक आवश्यकताओं और मौजूदा कानूनों की अपनी आधिकारिक व्याख्या पेश करता है। यह लागू कानूनों की व्याख्या प्रदान करता है, उनके दायरे और आवेदन की व्याख्या करता है, और यह सुनिश्चित करता है कि महिलाओं के कानूनी अधिकारों की रक्षा के लिए ऐसे कानूनों को प्रभावी ढंग से लागू किया जाए। सुप्रीम कोर्ट अपने निर्णयों के माध्यम से कानूनी प्रणाली में मिसाल कायम करने के लिए जिम्मेदार है, जिन्हें बाद में अन्य अदालतों और अन्य सरकारी निकायों के निर्णयों के आधार के रूप में उपयोग किया जाता है। ये मिसालें महिलाओं के खिलाफ किए जाने वाले साइबर अपराधों के लिए कानूनी मानदंड, परिभाषाएँ और उपाय निर्धारित करती हैं, जिससे इन अपराधों को संबोधित करने के तरीके में एकरूपता स्थापित

* Corresponding Author: **Neha Saxena**

Email: nehasaxena22181@gmail.com

Received 26 June. 2025; Accepted 16 July. 2025. Available online: 30 July. 2025.

Published by SAFE. (Society for Academic Facilitation and Extension)

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)



होती है। यह कानूनी ढाँचों के विश्लेषण और विकास में सक्रिय भूमिका निभाता है, यह सुनिश्चित करने के लिए काम करता है कि ये ढाँचे व्यापक हों और साइबर अपराध की हमेशा बदलती प्रकृति के अनुकूल होने में सक्षम हों।

सम्बन्धित साहित्य की समीक्षा:-

गिरि, डा. सविता आर. (2023)¹ ने अपने शोध पत्र 'भारत में साइबर अपराधों पर एक कानूनी अध्ययन: कानूनी ढाँचे को मजबूत करने के लिए मौजूदा कानूनों और रणनीतियों की पर्याप्तता का आकलन' में बताया कि सरकारें विधायी सुधार, अंतर्राष्ट्रीय सहयोग, क्षमता निर्माण, जन जागरूकता और नैतिक विचारों को शामिल करने वाले व्यापक दृष्टिकोण को अपनाकर, साइबर खतरों से बेहतर तरीके से निपट सकती हैं और डिजिटल पारिस्थितिकी तंत्र की अखंडता की रक्षा कर सकती हैं। शर्मा, सुनीता कुमारी (2022)² ने, 'ग्रामीण व शहरी शिक्षण प्रशिक्षणार्थियों की साइबर अपराध के प्रति जागरूकता का तुलनात्मक अध्ययन' नामक शीर्षक पर अध्ययन कार्य किया। अध्ययन निष्कर्ष में पाया गया कि ग्रामीण प्रशिक्षणार्थियों की जागरूकता का स्तर कम है वहीं शहरी प्रशिक्षणार्थियों की जागरूकता का स्तर ज्यादा है। भांगला, अपूर्वा एवं तुली, जानवी (2021)³ ने, 'A Study on Cyber Crime and its Legal Framework in India' विषय पर शोधपत्र प्रकाशित किया। साइबर-अपराध में मुख्य रूप से ऐसी गतिविधियाँ शामिल हैं जो किसी व्यक्ति की निजी जानकारी को प्रत्यक्ष या अप्रत्यक्ष रूप से निकालने के लिए एक उपकरण के रूप में इंटरनेट और कंप्यूटर का उपयोग करती हैं और व्यक्ति की सहमति के बिना या अवैध रूप से प्रतिष्ठा को कम करने या मानसिक या शारीरिक नुकसान पहुंचाने के उद्देश्य से इसे आनलाइन प्लेटफॉर्म पर प्रकट करती हैं। अलगांमदी, मोहम्मद आई. (2020)⁴ ने, 'A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide' विषय पर शोध पत्र प्रकाशित किया। शोध में अनुमान लगाया गया था कि साइबर अपराधियों के हाथों प्रति वर्ष छह ट्रिलियन डालर तक का नुकसान हो सकता है। कर्वे, डा. के.पी. एवं गुप्ता, डा. वीरेन्द्र सेन (2020) ने, "संचार साधनों की दौड़ में साइबर क्राइम की बढ़ती संख्या चिंता जागरूकता आवश्यक" विषय पर अध्ययन कार्य किया। साइबर क्राइम ऐसा है जो बिना किसी हथियार के किया जाता है और काफी घातक होता है। साइबर क्राइम मुख्यतः कंप्यूटर एवं मोबाइल के माध्यम से होता है। यहां संचार साधनों का दुरुपयोग कर अपराध किया जाता है इसके लिए किसी विशेष स्थल की जरूरत नहीं होती एक कमरे में बैठक भी अपराधी अपराध कर जाता है। बी.टी., श्रीमती चित्रा (2019) ने, Legal Regime of Cyber Crimes in India - A case study of Bangalore City with Special Reference to Cyber Crimes Against Women विषय पर पी-एच.डी. की उपाधि प्राप्त की। अध्ययन के निष्कर्ष

¹ Dr. Sarvita R. Giri (2023). 'A Legal Study on Cybercrimes in India: Assessing the Adequacy of Present Laws and Strategies for Strengthening Legal Frameworks'. *Social Sciecn Journal*, 13(4). 372-378. <https://resmilitaris.net/uploads/paper/09e503807f4a471a7fa036ab1820121f.pdf>

² शर्मा, सुनीता कुमारी (2022), "ग्रामीण व शहरी शिक्षण प्रशिक्षणार्थियों की साइबर अपराध के प्रति जागरूकता का तुलनात्मक अध्ययन" *International Journal of Creative Research Thoughts*, Vol. 10, Issue.5, pp: 19-22. <https://ijert.org/papers/IJCRT020004.pdf>

³ Bhangla, Apoorva & Tuli, Jahanvi (2021), "A Study on Cyber Crime and its Legal Framework in India", *Intenrational Journal of Law Management & Humanities*, Vol.4, Issue.2, pp: 493-504. <https://www.ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/>

⁴ Alghamdi, Mohammed I. (2020), "A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide", *International Journal of Engineering Research & Technology*, Vol.9, Issue.6, pp: 731-735. <https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide>

मे पाया गया कि सूचना प्रौद्योगिकी अधिनियम 2000 इलेक्ट्रॉनिक सूचना और डेटा के लिए उचित बौद्धिक संपदा संरक्षण से संबंधित नहीं है। आनलाइन कापीराइट, ट्रेडमार्क और पेटेंट से संबंधित विवादास्पद लेकिन बहुत महत्वपूर्ण मुद्दों पर कानून द्वारा ध्यान नहीं दिया गया है, जिससे कई खामियां निकल गई हैं। आईटी (संशोधन) अधिनियम, 2008 ने अधिकांश साइबर अपराधों के लिए सजा की मात्रा कम कर दी है। इसे सुधारने की आवश्यकता है और अधिकांश साइबर अपराधों को गैर-जमानती अपराध बनाने की आवश्यकता है।

साइबर अपराध की परिभाषा

सामान्य तौर पर साइबर अपराध को “कोई भी गैरकानूनी कार्य जिसमें कंप्यूटर या संचार उपकरण या कंप्यूटर नेटवर्क का उपयोग अपराध करने या अपराध को सुविधाजनक बनाने के लिए किया जाता है” के रूप में परिभाषित किया जा सकता है। नीचे कुछ साइबर अपराधों की सूची दी गई है, साथ ही उनके सांकेतिक स्पष्टीकरण भी दिए गए हैं। यह शिकायतों की बेहतर रिपोर्टिंग की सुविधा के लिए है।

साइबर अपराध को इस प्रकार परिभाषित किया जा सकता है, “अपराध जो जानबूझकर पीड़ित की प्रतिष्ठा को नुकसान पहुंचाने या आधुनिक दूरसंचार नेटवर्क का उपयोग करके प्रत्यक्ष या अप्रत्यक्ष रूप से पीड़ित को शारीरिक या मानसिक नुकसान पहुंचाने के लिए आपराधिक इरादे से व्यक्तियों या व्यक्तियों के समूहों के खिलाफ किए जाते हैं-जैसे इंटरनेट चैट रूम, ईमेल, नोटिस बोर्ड और मोबाइल फोन।” साइबर अपराध में इंटरनेट और कंप्यूटर का उपयोग शामिल है। यह किसी व्यक्ति की प्रतिष्ठा को कम करने और उन्हें प्रत्यक्ष या अप्रत्यक्ष रूप से शारीरिक या मानसिक नुकसान पहुंचाने के उद्देश्य से उनकी व्यक्तिगत या गोपनीय जानकारी को ऑनलाइन प्रकट या प्रकाशित करके उनकी गोपनीयता को खतरे में डालता है। साइबर अपराध दुनिया भर के लोगों के लिए खतरा बनता जा रहा है। महिलाएं आम तौर पर इन अपराधियों का निशाना होती हैं क्योंकि वे अनुभवहीन होती हैं और उन्हें साइबर दुनिया का ज्ञान नहीं होता है, जिससे वे तकनीकी सनक का शिकार हो जाती हैं।

देवराती हलदर और के. जयशंकर ने महिलाओं के खिलाफ साइबर अपराध को “इंटरनेट और मोबाइल फोन जैसे आधुनिक दूरसंचार नेटवर्क का उपयोग करके जानबूझकर पीड़ित को मनोवैज्ञानिक और शारीरिक रूप से नुकसान पहुंचाने के उद्देश्य से महिलाओं के खिलाफ लक्षित अपराध” के रूप में परिभाषित किया है।⁵

महिलाओं के विरुद्ध साइबर अपराध:

महिलाओं के प्रति साइबर अपराधों में ऑनलाइन उत्पीड़न, पीछा करना, धमकी देना, मानहानि, और यौन उत्पीड़न शामिल हैं। इसके अलावा, महिलाओं की तस्वीरें या वीडियो का दुरुपयोग, उनकी सहमति के बिना उन्हें ऑनलाइन प्रसारित करना, या उनके

⁵ <https://www.ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/>

साथ ऑनलाइन दुर्व्यवहार करना भी साइबर अपराध है। साइबर अपराधों में महिलाओं के खिलाफ कई तरह के अपराध होते हैं, जिनमें शामिल हैं:

- **साइबर उत्पीड़न:** महिलाओं को ऑनलाइन परेशान करना, धमकाना, या अपमानित करना। इसमें सोशल मीडिया पर अपमानजनक टिप्पणियां करना, अश्लील संदेश भेजना, या उन्हें ऑनलाइन बदनाम करना शामिल है।
- **साइबर स्टॉकिंग:** किसी महिला का पीछा करना, उसे लगातार ऑनलाइन संदेश भेजना, या उसकी गतिविधियों पर नजर रखना।
मानहानि: किसी महिला की प्रतिष्ठा को नुकसान पहुंचाने के लिए सोशल मीडिया या अन्य ऑनलाइन प्लेटफॉर्म पर झूठी और अपमानजनक जानकारी फैलाना।
- **यौन उत्पीड़न:** महिलाओं को ऑनलाइन यौन रूप से परेशान करना, जैसे कि अश्लील संदेश भेजना, अश्लील तस्वीरें या वीडियो साझा करना, या ऑनलाइन यौन शोषण करना।
- **पहचान की चोरी:** किसी महिला की निजी जानकारी जैसे कि उसका नाम, पता, या बैंक खाता नंबर चोरी करना और उसका दुरुपयोग करना।
- **बदला लेने वाला पोर्न:** किसी महिला की निजी तस्वीरें या वीडियो को उसकी सहमति के बिना ऑनलाइन प्रसारित करना।

ये कुछ सामान्य प्रकार के साइबर अपराध हैं जो महिलाओं के खिलाफ किए जाते हैं।

महिलाओं के विरुद्ध साइबर अपराधों के प्रति न्यायालय की भूमिका:

भारत में साइबर अपराधों से निपटने के लिए कई विधि हैं, मुख्य रूप से महिलाओं को यौन रूप से स्पष्ट सामग्री साझा करने और ऑनलाइन उत्पीड़न जैसे मुद्दों से बचाने के लिए। यहाँ महत्वपूर्ण विधायी इस प्रकार है –

- **सूचना प्रौद्योगिकी अधिनियम, 2000 (आईटी अधिनियम):** यह भारत में साइबर अपराधों को नियंत्रित करने वाला मुख्य कानून है। आईटी अधिनियम की धारा 66ई गोपनीयता उल्लंघन को संबोधित करती है, जिसमें किसी व्यक्ति की सहमति के बिना उसके निजी क्षेत्र की छवियों को कैप्चर करना, प्रकाशित करना या प्रसारित करना शामिल है। इसके अलावा, धारा 67 इलेक्ट्रॉनिक प्रारूपों में अनुचित सामग्री के वितरण या साझाकरण पर ध्यान केंद्रित करती है, जिसमें किसी भी उल्लंघन के लिए सख्त दंड लगाया जाता है। इस धारा ने स्पष्ट सामग्री के गैर-सहमति वितरण के खिलाफ महिलाओं की सुरक्षा में महत्वपूर्ण भूमिका निभाई है।
- **भारतीय संहिता (आईपीसी):** आईपीसी के विभिन्न भाग महिलाओं को लक्षित करने वाले साइबर अपराधों से संबंधित हैं। उदाहरण के लिए, धारा 354A यौन उत्पीड़न से संबंधित है, जिसमें यौन रूप से स्पष्ट सामग्री साझा करना शामिल है।

धारा 509 किसी भी शब्द, हाव-भाव या कृत्य को संबोधित करती है जिसका उद्देश्य किसी महिला की गरिमा को ठेस पहुँचाना है, जिसमें ऑनलाइन उत्पीड़न की स्थितियाँ भी शामिल हैं। इसके अतिरिक्त, धाराएँ 499 और 500 मानहानि को संबोधित करती हैं, जो उन स्थितियों में लागू होती हैं जहाँ महिलाओं के बारे में ऑनलाइन गलत जानकारी प्रसारित की जाती है।

- **घरेलू हिंसा से महिलाओं का संरक्षण अधिनियम, 2005:** यह अधिनियम मुख्य रूप से घरेलू हिंसा को संबोधित करता है, लेकिन इसमें ऑनलाइन उत्पीड़न भी शामिल हो सकता है जब यह घरेलू सेटिंग में होता है। यह महिलाओं को विभिन्न प्रकार के दुर्यवहारों के खिलाफ न्याय पाने का एक तरीका प्रदान करता है, जिसमें ऑनलाइन व्यवहार के परिणामस्वरूप होने वाली भावनात्मक और मनोवैज्ञानिक क्षति भी शामिल है।
- **कार्यस्थल पर महिलाओं का यौन उत्पीड़न (रोकथाम, निषेध और निवारण) अधिनियम, 2013:** यह कानून कार्यस्थल पर होने वाले ऑनलाइन उत्पीड़न पर लागू होता है। इसमें यौन उत्पीड़न से संबंधित मुद्दों को संभालने के लिए आंतरिक शिकायत समितियों के गठन की आवश्यकता होती है, जिसमें डिजिटल प्लेटफॉर्म के माध्यम से होने वाले उत्पीड़न भी शामिल हैं।
- **आपराधिक कानून (संशोधन) अधिनियम, 2013:** आपराधिक कानून (संशोधन) अधिनियम, 2013 3 फरवरी 2013 को एक अध्यादेश के माध्यम से लागू हुआ , और इसे भारत की संसद द्वारा पारित किए जाने के बाद 2 अप्रैल 2013 को आधिकारिक रूप से अधिनियमित किया गया । इस संशोधन ने यौन अपराधों के लिए कठोर दंड लाया और बलात्कार की परिभाषा को व्यापक बनाकर गैर-सहमति वाले डिजिटल कृत्यों को भी इसमें शामिल किया। यह ऑनलाइन होने वाली घटनाओं सहित विभिन्न प्रकार की यौन हिंसा के खिलाफ महिलाओं के लिए पूरी तरह से सुरक्षा प्रदान करने का प्रयास करता है।

साइबर अपराध प्रकोष्ठ:

इन कानूनों के साथ-साथ, कई राज्यों ने ऑनलाइन उत्पीड़न और महिलाओं को लक्षित करने वाले साइबर अपराधों से संबंधित मुद्दों से निपटने के उद्देश्य से विशेष साइबर अपराध इकाइयाँ बनाई हैं। ये प्रकोष्ठ ऐसे अपराधों में तेजी से प्रतिक्रिया और जांच करने में सक्षम बनाते हैं। भारत में मौजूदा कानूनी ढांचा विभिन्न प्रकार के साइबर अपराधों से निपटकर महिलाओं के लिए अधिक सुरक्षित ऑनलाइन स्थान को बढ़ावा देने का प्रयास करता है। फिर भी, इन कानूनों को ठीक से लागू करने और महिलाओं को उनके अधिकारों और उनके लिए उपलब्ध कानूनी विकल्पों के बारे में शिक्षित करने में अभी भी बाधाएं हैं। यह सुनिश्चित करने के लिए निरंतर समर्पण आवश्यक है कि ये विधि न केवल स्थापित हों बल्कि महिलाओं को ऑनलाइन अपराधों से बचाने के लिए प्रभावी ढंग से लागू भी हों।

साइबर उत्पीड़न के कारण;

साइबर उत्पीड़न के कई कारण हो सकते हैं:

- साइबर अपराधी आभासी दुनिया में अपने कार्यों के लिए सुरक्षित और कम जवाबदेह महसूस करते हैं, क्योंकि गुमनामी उन्हें अपराध करने के लिए प्रोत्साहित करती है।
- **विसंयम प्रभाव:** विसंयम प्रभाव के कारण लोग ऑनलाइन अलग तरह से व्यवहार कर सकते हैं, जैसा कि वे व्यक्तिगत रूप से नहीं करते। इससे लोग अधिक शत्रुतापूर्ण या हिंसक व्यवहार कर सकते हैं।
- **शक्ति असमानता:** कुछ लोग दूसरों पर प्रभाव डालने तथा उनके व्यवहार को नियंत्रित करने के लिए उन्हें ऑनलाइन परेशान कर सकते हैं।
- **सहानुभूति का अभाव:** साइबर अपराधियों में अन्य व्यक्तियों के प्रति सहानुभूति नहीं होती है और इसलिए वे लोगों पर उनके द्वारा किए जाने वाले प्रभाव की परवाह नहीं करते हैं और इस प्रकार वे साइबर उत्पीड़न में संलग्न होते हैं।
- **प्रतिशोध या प्रतिशोध:** दूसरों से बदला लेने के लिए, लोग साइबर अपराध में लिप्त हो जाते हैं और उस व्यक्ति को परेशान करते हैं जिसने उन्हें चोट पहुंचाई है या उनके साथ गलत किया है।
- **मनोवैज्ञानिक समस्या:** अवसाद या चिंता जैसी मानसिक स्वास्थ्य समस्या के कारण कुछ लोग साइबर उत्पीड़न में लिप्त हो जाते हैं। समाज और संस्कृति से प्रभाव: साइबर उत्पीड़न सामाजिक और सांस्कृतिक कारकों से भी प्रभावित हो सकता है, जैसे हानिकारक व्यवहार की स्वीकृति या विनम्र ऑनलाइन संचार के बारे में ज्ञान की कमी।
- **ईर्ष्या:** ईर्ष्या उन कारणों में से एक है जिसके कारण लोग पीछा करने का निर्णय लेते हैं, और यह वर्तमान और पिछले प्रेम संबंधों में प्रमुखता से देखा जाता है।

साइबर उत्पीड़न के प्रभाव;

1. ऑनलाइन उत्पीड़न से निपटना तथा ऐसे अपराधों के पीड़ितों को सहायता प्रदान करना अत्यंत महत्वपूर्ण है, ताकि इन नकारात्मक प्रभावों को रोका जा सके तथा सभी के लिए सुरक्षित वातावरण सुनिश्चित किया जा सके।
2. महिला सुरक्षा पर सोशल मीडिया का प्रभाव
3. सोशल मीडिया प्लेटफॉर्म के आने से हमारे संवाद करने के तरीके में बहुत बदलाव आया है, लेकिन इसने महिलाओं के खिलाफ नए तरह के अपराधों को भी जन्म दिया है। इन अपराधों में साइबरबुलिंग, ऑनलाइन उत्पीड़न, पीछा करना और निजी तस्वीरों का अनधिकृत वितरण शामिल है। इनमें से प्रत्येक मुद्दा अलग-अलग रूपों में सामने आता है, जो पीड़ितों और समाज दोनों के लिए बड़ी चुनौतियां पेश करता है।
4. साइबरबुलिंग ऑनलाइन नुकसान का एक आम रूप है। लोग अक्सर अपनी पहचान छिपाते हैं, महिलाओं के प्रति सीधे तौर पर चोट पहुंचाने वाली टिप्पणियां, धमकियां और धमकी देते हैं। यह सार्वजनिक पोस्ट, सीधे संदेश या यहां तक कि

संगठित कार्रवाइयों के माध्यम से हो सकता है जो तेजी से बढ़ सकते हैं। सोशल मीडिया पर जवाबदेही की कमी गलत काम करने वालों को प्रोत्साहित कर सकती है, जिससे उन्हें तत्काल नतीजों का सामना किए बिना हानिकारक तरीके से काम करने की अनुमति मिलती है।

5. ऑनलाइन उत्पीड़न एक महत्वपूर्ण चिंता का विषय है, जिसमें पीछा करना और लगातार अवांछित संचार शामिल है। महिलाओं को ऐसे व्यक्तियों का सामना करना पड़ सकता है जो सोशल मीडिया का उपयोग उनकी गतिविधियों पर नज़र रखने या परेशान करने वाले संदेश भेजने के लिए करते हैं। इससे भावनात्मक उथल-पुथल होती है और डिजिटल स्पेस और वास्तविक दुनिया दोनों में बेचैनी की भावना को बढ़ावा मिलता है। इस तरह के उत्पीड़न का भावनात्मक प्रभाव गहरा और स्थायी हो सकता है।
6. निजी छवियों का अनधिकृत वितरण, जिसे आमतौर पर रिवेंज पोर्न के रूप में जाना जाता है, एक बहुत ही हानिकारक कार्य है जो सोशल मीडिया के विकास के साथ और अधिक प्रमुख हो गया है। व्यक्ति बिना अनुमति के निजी छवियों को वितरित कर सकते हैं, जिसके परिणामस्वरूप प्रभावित लोगों की प्रतिष्ठा को नुकसान पहुँचता है और उन्हें काफी भावनात्मक पीड़ा होती है। यह क्रिया विभिन्न प्लेटफ़ॉर्म पर तेजी से फैल सकती है, जिससे व्यक्तियों के लिए अपनी व्यक्तिगत छवियों पर नियंत्रण पुनः प्राप्त करने की प्रक्रिया जटिल हो जाती है।

इन अपराधों के बारे में बढ़ती जागरूकता के बावजूद, ऐसे अपराधों के खिलाफ़ कानूनी कार्रवाई करने में उल्लेखनीय कठिनाइयाँ हैं। एक महत्वपूर्ण चिंता जिम्मेदार लोगों की छिपी हुई पहचान है। इंटरनेट पर गुमनाम रहने की क्षमता अपराधियों की पहचान करना और उन्हें पकड़ना चुनौतीपूर्ण बनाती है, क्योंकि कई सोशल मीडिया प्लेटफ़ॉर्म उपयोगकर्ताओं को उनकी वास्तविक पहचान का खुलासा किए बिना खाते बनाने की अनुमति देते हैं। पहचान की यह कमी हानिकारक कार्यों में भाग लेने वाले व्यक्तियों के लिए स्वतंत्रता की भावना को बढ़ावा दे सकती है।

एक और चुनौती यह है कि पीड़ितों को अक्सर अपने कानूनी अधिकारों या न्याय पाने के लिए उनके पास उपलब्ध विकल्पों के बारे में पता नहीं होता है। कई पीड़ित इस बारे में अनिश्चित महसूस कर सकते हैं कि घटनाओं की रिपोर्ट कैसे करें या बोलने के परिणामों के बारे में चिंता कर सकते हैं, जिसके परिणामस्वरूप रिपोर्ट किए गए अपराधों की कमी होती है। क्षेत्राधिकार संबंधी मुद्दे जटिलता को बढ़ाते हैं, क्योंकि सोशल मीडिया वैश्विक स्तर पर काम करता है, जिससे सीमा पार अपराधों के मामलों में किस देश के कानून प्रासंगिक हैं, इस बारे में जटिल कानूनी प्रश्न उठते हैं।

इसके अलावा, कानून प्रवर्तन एजेंसियों को प्रौद्योगिकी से संबंधित कठिनाइयों का सामना करना पड़ सकता है। प्रौद्योगिकी की तीव्र प्रगति अक्सर इन अपराधों को संबोधित करने के लिए बनाए गए कानूनी ढाँचों को पार कर जाती है। नतीजतन, जांचकर्ताओं के पास साइबर अपराधों से प्रभावी ढंग से निपटने के लिए उचित प्रशिक्षण या संसाधन नहीं हो सकते हैं। सामाजिक बाधाएँ प्रगति में बाधा डाल सकती हैं, क्योंकि इन घटनाओं की रिपोर्टिंग से जुड़ी नकारात्मक धारणाएँ पीड़ितों, विशेष रूप से महिलाओं को सहायता के लिए आगे आने से हतोत्साहित कर सकती हैं।

संक्षेप में, हालांकि सोशल मीडिया प्लेटफॉर्म संपर्क और आत्म-अभिव्यक्ति के लिए नए रास्ते प्रदान करते हैं, लेकिन वे महिलाओं के खिलाफ नए प्रकार के अपराधों को भी सक्षम बनाते हैं। इन अपराधों पर मुकदमा चलाने में आने वाली कठिनाइयाँ डिजिटल युग में इन मुद्दों से प्रभावी ढंग से निपटने के लिए गहन कानूनी सुधारों, पीड़ितों के बीच अधिक जागरूकता और कानून प्रवर्तन के लिए बेहतर प्रशिक्षण की तत्काल आवश्यकता को उजागर करती हैं।

महिलाओं के विरुद्ध साइबर अपराध पर अंतर्राष्ट्रीय परिप्रेक्ष्य

साइबर अपराधों के प्रति भारत का न्यायिक दृष्टिकोण पिछले कुछ वर्षों में उल्लेखनीय रूप से बदला है, खासकर सूचना प्रौद्योगिकी अधिनियम, 2000 और उसके बाद के संशोधनों के कार्यान्वयन के साथ। फिर भी, अन्य देशों की तुलना में, विभिन्न अंतर और प्रभावी दृष्टिकोण देखे जा सकते हैं।

भारत में, कानूनी ढांचा मुख्य रूप से साइबर अपराधों की रूपरेखा तैयार करने और दंड निर्धारित करने पर केंद्रित है। हालांकि आईटी अधिनियम आधारभूत कार्य करता है, लेकिन इसे व्यवहार में लाना मुश्किल साबित होता है क्योंकि कानून प्रवर्तन और न्यायिक अधिकारियों के पास अक्सर आवश्यक विशेष प्रशिक्षण का अभाव होता है। इसके अलावा, कानूनी प्रक्रियाओं की क्रमिक प्रगति प्रभावित लोगों के लिए त्वरित न्याय में बाधा डाल सकती है।

इसकी तुलना में, संयुक्त राज्य अमेरिका और यूनाइटेड किंगडम जैसे देशों ने साइबर अपराधों से निपटने के लिए अधिक गहन प्रणालियाँ स्थापित की हैं। अमेरिका में कंप्यूटर धोखाधड़ी और दुरुपयोग अधिनियम के साथ-साथ कानून प्रवर्तन में विभिन्न विशेष इकाइयाँ हैं जो साइबर अपराधों पर ध्यान केंद्रित करती हैं। ये इकाइयाँ अक्सर तकनीकी कंपनियों और वैश्विक संगठनों के साथ मिलकर काम करती हैं, जिससे अपराधियों की कुशलतापूर्वक जाँच करने और उन पर मुकदमा चलाने की उनकी क्षमता में सुधार होता है। यूके ने आगे की सोच वाला रुख अपनाया है, जिसमें राष्ट्रीय साइबर अपराध इकाई साइबर खतरों से निपटने के लिए स्थानीय पुलिस बलों के साथ मिलकर काम कर रही है।

एक प्रभावी दृष्टिकोण जिसे भारत इन देशों से अपना सकता है, वह है समर्पित साइबर अपराध इकाइयों का निर्माण करना, जिनके पास आवश्यक तकनीकी कौशल हों। डिजिटल फॉरेंसिक और साइबर कानून में कानून प्रवर्तन कर्मियों को शिक्षित करने से जांच के परिणामों में काफी सुधार हो सकता है। इसके अतिरिक्त, सरकारी निकायों, निजी कंपनियों और वैश्विक भागीदारों के बीच सहयोग को प्रोत्साहित करने से साइबर अपराध के प्रति प्रतिक्रियाओं की दक्षता में सुधार हो सकता है।

एक और सबक यह है कि लोगों में जागरूकता बढ़ाना और समझ को बढ़ावा देना कितना महत्वपूर्ण है। साइबर अपराधों से प्रभावी तरीके से निपटने वाले देश अक्सर नागरिकों को ऑनलाइन सुरक्षा और घटनाओं की रिपोर्ट करने के तरीके के बारे में जानकारी देने की पहल पर ध्यान केंद्रित करते हैं। यह दृष्टिकोण न केवल व्यक्तियों का समर्थन करता है बल्कि अधिक पीड़ितों को बोलने के लिए प्रेरित करता है, जिससे कानून प्रवर्तन को इन अपराधों से प्रभावी ढंग से निपटने के लिए आवश्यक जानकारी मिलती है।

आइसलैंड के राष्ट्रपति गुडनी टी. जोहान्सन ने सम्मेलन के प्रतिभागियों को संबोधित करते हुए लैंगिक समानता और ऑनलाइन हिंसा से लड़ने के लिए आगे प्रगति की आवश्यकता पर बल दिया। महिलाओं के खिलाफ हिंसा और घरेलू हिंसा के खिलाफ कार्रवाई पर यूरोपीय परिषद के विशेषज्ञों के समूह (GREVIO) ने 2021 में महिलाओं के खिलाफ हिंसा के डिजिटल आयाम पर इस्तांबुल कन्वेंशन के सदस्य देशों के लिए एक सिफारिश विकसित की, ताकि डिजिटल क्षेत्र में महिलाओं के खिलाफ हिंसा के लिए संधि के प्रावधानों के आवेदन पर मार्गदर्शन प्रदान किया जा सके। बुडापेस्ट कन्वेंशन और इलेक्ट्रॉनिक साक्ष्य के प्रकटीकरण और सहयोग बढ़ाने पर इसका दूसरा अतिरिक्त प्रोटोकॉल अपराधों की जांच करने और सीमा पार साक्ष्य प्राप्त करने और न केवल ऑनलाइन किए गए अपराधों पर, बल्कि उन सभी अपराधों से निपटने में आवश्यक अंतर्राष्ट्रीय सहयोग सुनिश्चित करने के लिए उपकरण प्रदान करता है, जिनमें इलेक्ट्रॉनिक साक्ष्य शामिल हैं। महासचिव ने कहा, "साइबर अपराध और महिलाओं के खिलाफ हिंसा से निपटने के लिए इन दोनों उपकरणों का उपयोग करना आवश्यक है - ताकि महिलाओं के लिए ऑनलाइन सबसे सुरक्षित वातावरण सुनिश्चित किया जा सके।

भारतीय परिपेक्ष में

गैर-सरकारी संगठन पासुमई त्यागम का प्रतिनिधित्व कर रही सौम्या अंबुमणि ने शनिवार को यहां कहा कि महिला जांच अधिकारी और पॉक्सो मामलों के लिए महिलाओं के लिए विशेष अदालतें तथा साइबर अपराध अदालतें समय की मांग हैं। सुश्री सौम्या ने मद्रास विश्वविद्यालय में आयोजित छठे अंतर्राष्ट्रीय और 45वें अखिल भारतीय अपराध विज्ञान सम्मेलन में एक सत्र की अध्यक्षता की और सरकार से अपील की कि वह सूचना एवं प्रौद्योगिकी अधिनियम 2000 के तहत आपत्तिजनक सामग्री और वेबसाइट को तत्काल हटाये। उन्होंने परिवार, पुलिस और न्यायपालिका द्वारा पीड़ितों की पहचान और गोपनीयता की रक्षा करने का आह्वान किया। उन्होंने कहा कि आईटी अधिनियम केवल ई-कॉमर्स और वित्तीय संस्थानों को साइबर अपराध हमलों से बचाता है, जबकि महिलाओं के खिलाफ इंटरनेट अपराधों पर कम चर्चा होती है और उन्हें संबोधित करने के लिए कम प्रयास किए जाते हैं। महिलाओं का अभद्र चित्रण (निषेध अधिनियम 1986) महिलाओं के अभद्र चित्रण वाले प्रकाशनों और विज्ञापनों पर प्रतिबंध लगाता है।

राष्ट्रीय महिला आयोग ने आज नई दिल्ली में महिलाओं के लिए डिजिटल शक्ति अभियान के अंतर्गत डिजिटल शक्ति केंद्र का उद्घाटन किया। इस केन्द्र का उद्देश्य साइबर अपराधों के बारे में जागरूकता बढ़ाना है। यह केंद्र शिकायतों को दर्ज करने और उनके निपटान में तकनीकी सहायता प्रदान करेगा। आयोग ने कहा है कि डिजिटल अपराधों में वृद्धि को देखते हुए यह पहल महिलाओं को डिजिटल दुनिया में खुद की सुरक्षा करने और सशक्त बनाने में मदद करेगी। यह केंद्र साइबर अपराध की शिकायतों का समय पर और प्रभावी रूप से समाधान सुनिश्चित करेगा।

डिजिटल शक्ति केंद्र का उद्घाटन राष्ट्रीय महिला आयोग की अध्यक्ष सुश्री रेखा शर्मा ने साइबर पीस फाउंडेशन के सहयोग से किया है। इस दौरान सभा को संबोधित करते हुए सुश्री शर्मा ने कहा कि भारत में साइबर अपराध के मामलों में वृद्धि हुई है। देश में

वर्ष 2021 में 52 हजार 9 सौ 74 साइबर अपराध से जुड़े मामले दर्ज किए गए थे, जो वर्ष 2022 में बढ़कर 65 हजार 8 सौ 93 हो गए।

न्यायिक निर्णय:

श्रेया सिंघल बनाम भारत संघ (2015)

श्रेया सिंघल बनाम भारत संघ (2015) का मामला भारत के सर्वोच्च न्यायालय द्वारा दिया गया एक महत्वपूर्ण निर्णय है, जिसने इंटरनेट के संबंध में भाषण और अभिव्यक्ति की स्वतंत्रता से संबंधित कानूनी ढांचे को काफी प्रभावित किया। यह स्थिति तब उत्पन्न हुई जब कानून की छात्रा श्रेया सिंघल ने सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 66 ए की संवैधानिकता पर सवाल उठाया। इस धारा ने सोशल मीडिया सहित संचार सेवाओं के माध्यम से "आक्रामक" संदेश भेजना अवैध बना दिया और अस्पष्ट मानकों के आधार पर व्यक्तियों की गिरफ्तारी की अनुमति दी। इस प्रावधान को इसके व्यापक दायरे और दुरुपयोग की संभावना के कारण आलोचना का सामना करना पड़ा, जिसके परिणामस्वरूप मनमाने ढंग से गिरफ्तारियाँ हुईं, खासकर राजनीतिक असहमति और ऑनलाइन आलोचना से संबंधित स्थितियों में। सर्वोच्च न्यायालय ने सर्वसम्मति से निर्णय देते हुए धारा 66A को असंवैधानिक घोषित किया। न्यायालय ने निर्धारित किया कि यह प्रावधान भारतीय संविधान के अनुच्छेद 19(1)(a) का उल्लंघन करता है, जो अभिव्यक्ति की स्वतंत्रता के अधिकार को सुनिश्चित करता है।

कृष्ण कुमार बनाम उत्तर प्रदेश राज्य (2021)

कृष्ण कुमार बनाम उत्तर प्रदेश राज्य (2021) का मामला इलाहाबाद उच्च न्यायालय का एक महत्वपूर्ण फैसला है, जिसने बिना सहमति के अंतरंग छवियों को साझा करने के गंभीर मुद्दे से निपटा, जिसे आमतौर पर "रिवेंज पोर्न" के रूप में जाना जाता है। यह स्थिति तब सामने आई जब कृष्ण कुमार पर एक महिला की निजी तस्वीरों उसकी अनुमति के बिना वितरित करने के आरोप लगे। पीड़िता ने एक शिकायत दर्ज कराई, जिसमें उसकी निजता के उल्लंघन और उसकी तस्वीरों के अनधिकृत साझाकरण से होने वाली भावनात्मक उथल-पुथल पर जोर दिया गया। इस स्थिति ने निजी सामग्री के अनधिकृत साझाकरण के खिलाफ कानूनी सुरक्षा उपायों की तत्काल आवश्यकता को उजागर किया, जो डिजिटल संचार के विकास के साथ अधिक आम हो गया है। इलाहाबाद उच्च न्यायालय ने पीड़िता के पक्ष में फैसला सुनाते हुए कहा कि बिना सहमति के अंतरंग तस्वीरें साझा करना निजता का उल्लंघन है। न्यायालय ने सूचना प्रौद्योगिकी अधिनियम की धारा 66ई का हवाला दिया, जो निजता के उल्लंघन और किसी व्यक्ति के निजी अंगों की तस्वीरों को अनधिकृत रूप से कैप्चर करने, प्रकाशित करने या साझा करने से संबंधित है। इलाहाबाद उच्च न्यायालय ने पीड़िता के पक्ष में फैसला सुनाते हुए कहा कि बिना सहमति के अंतरंग तस्वीरें साझा करना निजता का उल्लंघन है। न्यायालय ने सूचना प्रौद्योगिकी अधिनियम की धारा 66ई का हवाला दिया, जो निजता के उल्लंघन और किसी व्यक्ति के निजी अंगों की तस्वीरों को अनधिकृत रूप से कैप्चर करने, प्रकाशित करने या साझा करने से संबंधित है।

एक्स बनाम तेलंगाना राज्य (2021)

एक्स बनाम तेलंगाना राज्य (2021) का मामला तेलंगाना उच्च न्यायालय द्वारा एक महत्वपूर्ण निर्णय के रूप में सामने आया है, जो ऑनलाइन उत्पीड़न के महत्वपूर्ण मामले पर ध्यान केंद्रित करता है, विशेष रूप से महिलाओं की संशोधित छवियों के वितरण से संबंधित। इस स्थिति में, "X" के नाम से जानी जाने वाली व्यक्ति को ऑनलाइन उत्पीड़न का सामना करना पड़ा क्योंकि उसकी बदली हुई तस्वीरें कई प्लेटफॉर्म पर शेयर की गईं। इस कार्रवाई ने न केवल उसकी निजता का उल्लंघन किया, बल्कि काफी भावनात्मक और मनोवैज्ञानिक उथल-पुथल भी पैदा की। पीड़िता ने न्याय की मांग की, जिम्मेदार लोगों के खिलाफ त्वरित कार्रवाई की तत्काल आवश्यकता पर जोर दिया। तेलंगाना उच्च न्यायालय ने पीड़िता का समर्थन करते हुए उसके साथ हुए उत्पीड़न की गंभीरता को स्वीकार किया।

रवि बनाम कर्नाटक राज्य (2022)

रवि बनाम कर्नाटक राज्य (2022) मामला कर्नाटक उच्च न्यायालय का एक महत्वपूर्ण फैसला है जो सोशल मीडिया प्लेटफॉर्म पर साइबर धमकी और उत्पीड़न के गंभीर मुद्दे से निपटता है। यह स्थिति तब सामने आई जब याचिकाकर्ता रवि पर सोशल मीडिया पर अपमानजनक टिप्पणी और धमकियाँ देकर एक महिला के प्रति ऑनलाइन उत्पीड़न में भाग लेने का आरोप लगा। पीड़िता ने कानूनी कार्रवाई की और दावा किया कि इस व्यवहार ने उसकी गरिमा और व्यक्तिगत सुरक्षा का उल्लंघन किया है। कर्नाटक उच्च न्यायालय ने एक निर्णय जारी किया जिसमें ऑनलाइन उत्पीड़न से संबंधित कई महत्वपूर्ण पहलुओं पर प्रकाश डाला गया।

एन.सी.आर.बी.वार्षिक रिपोर्ट, 2020

रिपोर्ट के अनुसार, वर्ष 2020 के दौरान भारत में होने वाले कुल साइबर अपराधों में से 20 प्रतिशत महिलाओं के खिलाफ हुए, जिसमें साइबर धोखाधड़ी के बाद 'यौन शोषण' के सर्वाधिक मामले दर्ज हुए, जो साइबर अपराध से जुड़ी मंशा को स्पष्ट करता है।

साइबर अपराध से संबंधित मामलों में प्राथमिकी दर-

- अनुचित यौन सामग्री के प्रकाशन या प्रसारण के लिये 47.1 प्रतिशत
- साइबर ब्लैकमेलिंग और धमकी के मामलों में 66.7 प्रतिशत
- साइबर स्टार्किंग और महिलाओं एवं बच्चों को डराने-धमकाने के मामलों में 27.6 प्रतिशत
- फ़र्जी प्रोफाइल के केवल दो मामलों में ट्रायल पूरा हुआ, जबकि 148 मामले लंबित हैं।
- गृह मंत्रालय वर्ष 2018 से राष्ट्रीय साइबर अपराध पोर्टल का संचालन कर रहा है। इस पर वर्ष 2021 में महिलाओं के खिलाफ 600,000 से अधिक शिकायतें प्राप्त हुईं, जिनमें से केवल 12,776 मामलों में ही प्राथमिकी दर।

निष्कर्ष:

हालाँकि भारत ने महिलाओं को लक्षित करने वाले साइबर अपराधों से निपटने के लिए एक संपूर्ण कानूनी संरचना बनाई है, फिर भी इन कानूनों को ठीक से लागू करने और प्रभावित लोगों को न्याय दिलाने में अभी भी बाधाएँ हैं। न्यायिक दृष्टिकोण को प्रौद्योगिकी में तेज़ बदलावों और साइबर अपराधों की बढ़ती जटिलता के अनुकूल होने की आवश्यकता है। इसमें कानून प्रवर्तन एजेंसियों के भीतर जागरूकता बढ़ाना, साइबर अपराध के मामलों के प्रबंधन के लिए उचित प्रशिक्षण देना और पीड़ितों के लिए आगे आकर घटनाओं की रिपोर्ट करने के लिए स्वागत योग्य माहौल बनाना शामिल है। इसके अलावा, नई चुनौतियों से निपटने और ऑनलाइन वातावरण में महिलाओं के लिए मजबूत सुरक्षा सुनिश्चित करने के लिए मौजूदा कानूनों का निरंतर मूल्यांकन और समायोजन महत्वपूर्ण है। अंत में, महिलाओं के लिए अधिक सुरक्षित ऑनलाइन स्थान को बढ़ावा देने और साइबर अपराधों के खिलाफ उनके अधिकारों की रक्षा करने के लिए न्यायपालिका, कानून प्रवर्तन और समुदाय के बीच मिलकर काम करना आवश्यक है। नागरिकों द्वारा साइबर अपराध की त्वरित रिपोर्टिंग, फॉरेंसिक तकनीक का उपयोग करते हुए पुलिस द्वारा तकनीकी रूप से कुशल जाँच और न्यायालय की कार्यवाही का समयबद्ध समापन साइबर अपराधियों को पकड़ने के लिये आवश्यक है। निष्कर्ष के तौर पर, हालाँकि भारत ने साइबर अपराधों से निपटने में प्रगति की है, लेकिन इसमें और सुधार की संभावना बनी हुई है। लक्षित प्रशिक्षण, टीमवर्क और सामुदायिक जागरूकता प्रयासों सहित अधिक विकसित प्रणालियों वाले देशों की प्रभावी रणनीतियों को अपनाकर, भारत साइबर अपराधों के प्रति अपनी न्यायिक प्रतिक्रिया में सुधार कर सकता है और अपने नागरिकों की अधिक प्रभावी ढंग से सुरक्षा कर सकता है।

- वास्तविक अपराधों की तुलना में प्राथमिकी दर काफी कम हैं। साइबर अपराधों के त्वरित परीक्षण से प्राथमिकी दर बेहतर की जा सकती है। आई टी अधिनियम की धारा 67, 67A और 67B विशेष प्रकार के यौन अपराधों, जैसे- इंटरनेट पर बच्चों एवं महिलाओं को यौन कार्य के लिये तैयार करने एवं उन्हें प्रेरित करने को कवर नहीं करता है। अधिनियम में इस संदर्भ में संशोधन करने और धारा 67 और 67A में उपबंधित 'नैतिक ढाँचे' को हटाने और 'सहमति के तत्व' को जोड़ने की आवश्यकता है।
- व्यक्तिगत डाटा संरक्षण विधेयक में महिलाओं से संबंधित डाटा की विशेष सुरक्षा का उपबंध जोड़ा जाना चाहिये। साइबर अपराधों से संबंधित अभियोजकों और न्यायिक अधिकारियों के व्यवस्थित प्रशिक्षण से मुकदमे दर्ज करने और उनके निपटान में तेजी आएगी।
- साइबर अपराध और सुरक्षा के बारे में जागरूकता बढ़ाने के लिये युवा, विशेषकर, बालिकाओं और महिलाओं को भी सर्फिंग करते समय उचित सावधानी बरतने की आवश्यकता है।
- साइबर दुरुपयोग और उपलब्ध सुरक्षा उपायों के बारे में छात्रों को शिक्षित करने में स्कूलों, कॉलेजों, विश्वविद्यालयों और समुदायों को बड़े पैमाने पर सक्रिय भूमिका निभानी चाहिये।

- सोशल मीडिया प्लेटफॉर्म को शामिल कर उन्हें अपमानजनक ट्रैफिक की निगरानी और जांच करने के लिये प्रोत्साहित करना चाहिये एवं उपयोगकर्ताओं, विशेष रूप से महिलाओं और बच्चों के लिये अधिक सुरक्षा उपाय बनाने के लिये प्रेरित करना चाहिये।
- केंद्र सरकार ने 'साइबर क्राइम प्रिवेंशन अगेंस्ट वूमेन एंड चिल्ड्रन' (CCPWC) योजना के तहत राज्यों और केंद्र शासित प्रदेशों को 'साइबर फोरेंसिक-सह-प्रशिक्षण प्रयोगशालाएँ' शुरू करने के लिये वित्त आबंटित किया है। राज्यों को भी अपनी फोरेंसिक इकाइयों के लिये संसाधन आबंटित करने की आवश्यकता है।

संदर्भ सूची:

- भारत सरकार, सूचना प्रौद्योगिकी अधिनियम, 2000
- भारतीय दंड संहिता, 1860 (IPC)
- पॉक्सो अधिनियम, 2012 (बाल यौन अपराधों से संरक्षण अधिनियम)
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (MHA द्वारा) – साइबर अपराध की रिपोर्ट करने हेतु सरकारी पोर्टल
- राष्ट्रीय महिला आयोग
- इलेक्ट्रॉनिक एवं सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार
- एनसीआरबी रिपोर्ट – साइबर अपराध से संबंधित आँकड़े

विधि आयोग की रिपोर्टें

- प्रीति राज, महिलाओं के खिलाफ साइबर अपराध , क्लियरआईएस (21 अक्टूबर, 2022), <https://www.clearias.com/cybercrime-against-women/?srsltid=AfmBOopIezCKSiCxz5BWz0onglKHukAmO2XkuNPERBtEZDccUD6gxaKX> .
- डेल, (10 दिसंबर, 2023), <https://www.ijfans.org/uploads/paper/374cf990d6568e78319acc782da11df2.pdf> .
- धृति एम कपाड़िया, भारत में महिलाओं के खिलाफ साइबर अपराध और कानून , (21 नवंबर, 2018), <https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india> .

- भारतीय परवरिश में साइबरस्पेस के तहत महिलाओं का उत्पीड़न , (3 जुलाई, 2017), https://docs.manupatra.in/newsline/articles/Upload/786274E9-B397-4610-8912-28D6D03230F9.monika_jain_pdf_1-1111.pdf `