Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0057

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

साइबर अपराध तथा पेशेवर सामाजिक कार्य हस्तक्षेप

माधवी बापुराव धुर्वे
ई - मेल : madhavi0712dhurve@gmail.com
मो. नं. : 9527983753

साइबर अपराध **(Cyber Crime)** वह एक ऐसी गतिविधि या अपराध होते हैं जिनका प्रयोग कंप्यूटर, इंटरनेट, मोबाइल या अन्य डिजिटल तकनीकों का उपयोग मान्य कानून का उल्लंघन हेतु किया जाता हैं। इन अपराधों में आंकडों की चोरी **(Data Theft)**, जानकारी में फेरबदल **(Data Alteration),** जानकारी को नष्ट करना **(Data Destruction),** हैकिंग **(Hacking)**, वित्तीय धोखाधड़ी(Financial fraud), पहचान की चोरी(Identity Theft), ऑनलाइन उत्पीड़न**(Online Harassment)**, स्पैम या वाइरस **(Spam and Virus)** की मदद से सिस्टम की सुरक्षा को खंडित करना(Dismantling security), साइबर फिशिंग **(Cyber Phishing)**, साइबर बुलीइंग **(Cyber Bullying)**, डाटा चोरी**(Data Theft)**, और अन्य डिजिटल तरीकों **(Digital Methods)**से अपराध करना शामिल होता है। साइबर अपराधी आमतौर पर इंटरनेट का उपयोग करते हुए कंप्यूटर नेटवर्क या सिस्टम में अनधिकृत तरीके**(Unauthorized methods)** से घुसपैठ डिजिटल दुनिया में करतें हैं। जिससे व्यक्तिगत**(personal),** वित्तीय**(financial),** और गोपनीय जानकारी का नुकसान**(Loss of confidential information)** हो सकता है। इसके कई प्रकार हो सकतें हैं जैसे कि जानकारी चोरी करना, जानकारी मिटाना, जानकारी मे फेर बदल करना, किसी कि जानकारी को किसी और को देना या कंप्यूटर मे उपयोगी भाग को चोरी करना या नष्ट करना, किसी पर हर वक़्त नजर रखना। आम तौर पर साइबर अपराध के प्रकारों में, जानकारी की चोरी करना जैसे किसी के भी कंप्यूटर से उसकी निजी जानकारी निकालना, उपयोगकर्ता नाम या पासवर्ड का दुरुपयोग करना। जानकारी मिटाना ताकी उसे नुकसान हो या कोई जरूरी जानकारी को नष्ट कर देना, फेर बदल करना, जानकारी मे कुछ हटाना या जोड़ना या उस जानकारी के अर्थ को बदल देना। बाहरी नुकसान या डिवाइस को आंतरिक रूप से नष्ट करना, उसे तोडना या उसकी चोरी करना भी साइबर अपराध के अंतर्गत आता है। स्पैम ईमेल का प्रयोग करके कंप्यूटर को नुकसान पहुचाना। हैकिंग द्वारा किसी की भी निजी जानकारी को हैक करना। साइबर फिशिंग के तहत किसी के पास स्पैम ईमेल भेजना ताकी वो अपनी निजी जानकारी दे और उस जानकारी से उसका नुकसान हो सके क्योकि यह ईमेल लोगों को आकर्षित करतें है जिस कारण लोग इसका शिकार हो जातें हैं। वायरस की मदद से साइबर अपराधी कुछ ऐसे सॉफ्टवेयर कम्प्युटर पर भेजते हैं जिसमें वायरस छिपे होते हैं, इनमें नेटवर्क वायरस, फ़ाइल इंफेक्टर वायरस, बूट सेक्टर वायरस और मल्टीपार्टाइट वायरस, लव, वर्म, टार्जन हॉर्स, लॉजिक हॉर्स आदि वायरस शामिल हो सकतें हैं, यह कंप्यूटर को काफी हानिकारक होते हैं। सॉफ्टवेयर पाइरेसी **(Software Piracy)**द्वारा सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है। फर्जी बैंक कॉल, ईमेल, मैसेज **(Fake Bank Calls, Emails, and Messages)** भेजकर एटीएम नंबर और पासवर्ड की चोरी करना, धमकी देना, भ्रामक सूचना फैलाना। सोशल नेटवर्किंग साइटों पर अफवाह फैलाना **(Threats and Spreading False Information)**, साइबर बुलिंग करना आदि साइबर अपराध के तहत दर्ज किये जातें हैं।

साइबर अपराध के विषय में भारत सरकार ने **Information Technology Act, 2000 (IT Act, 2000)** पारित किया जिसमें विशेष रूप से साइबर अपराधों को परिभाषित किया है। इस कानून के तहत साइबर अपराधों से संबंधित कई धाराएं निर्धारित की गई हैं, जो कंप्यूटर और नेटवर्क आधारित अपराधों की पहचान करती हैं और उनकी सजा भी तय करती हैं। यह कानून भारत में साइबर अपराधों और इलेक्ट्रॉनिक लेन-देन की सुरक्षा के लिए एक कानूनी ढांचा प्रदान करता है। इस कानून को समय-समय पर संशोधित किया गया है ताकि यह बदलती तकनीकी और डिजिटल चुनौतियों का मुकाबला कर सके। वर्ष **2008 में** इस अधिनियम में महत्वपूर्ण संशोधन किए गए थे। इस संशोधन ने कुछ नए अपराधों को शामिल किया, जैसे कि साइबर धोखाधड़ी, डेटा चोरी, और व्यक्तिगत जानकारी की सुरक्षा से जुड़े अपराध। आधिकारिक इलेक्ट्रॉनिक दस्तावेजों की वैधता **(Validity of Official Electronic Documents),** आधिकारिक डिजिटल हस्ताक्षर **(Official Digital Signature)** को कानूनी रूप से मंजूरी। इस संशोधन में **साइबर अपराध** के तहत नई श्रेणियाँ जोड़ी गईं, जैसे कि साइबर बुलीइंग, साइबर धोखाधड़ी, और इलेक्ट्रॉनिक संदेशों के माध्यम से उत्पीड़न का चिन्हिकरण **(Marking Harassment Through Electronic Messages)**। **साइबर सुरक्षा (Cyber Security)** के लिए प्राधिकृत निकायों **CERT-In (Computer Emergency Response Team-In)** की स्थापना। कंप्यूटर

संसाधनों की हानि, हैकिंग, साइबर स्टॉकिंग **(Cyber Stalking),** और साइबर बुलीइंग जैसे अपराधों के लिए कड़ी सजा का प्रावधान किया गया। अगला संशोधन **IT (Amendment) Act, 2018 (Proposed but not yet enacted)** इस संशोधन ने डेटा प्राइवेसी और सुरक्षा **(Data Privacy And Security)** को और अधिक सख्त किया। इसके तहत डेटा सुरक्षा उल्लंघन के लिए ज़्यादा सजा का प्रावधान था, लेकिन इसे अभी तक पूरी तरह से लागू नहीं किया गया है। प्रमुख संशोधनों के उद्देश्य साइबर अपराधों और साइबर सुरक्षा में सुधार। इलेक्ट्रॉनिक दस्तावेजों **(Electronic Documents)** की वैधता और स्वीकार्यता **(Validity and Admissibility)** बढ़ाना। निजता की रक्षाऔर सुरक्षा **(Protect and Safeguard Privacy)** के लिए कानूनी कदम उठाना। इन संशोधनों ने **IT Act** को समय के साथ और भी अधिक प्रभावी बनाया जाना है, ताकि डिजिटल युग के विकसित होते खतरों और कानूनी चुनौतियों का मुकाबला किया जा सके।

साइबर अपराध के नियंत्रण हेतु पेशेवर सामाजिक कार्य हस्तक्षेप- साइबर अपराध एक जटिल और तात्कालिक तेजी से बढ़ती हुई समस्या है, जो वर्तमान में महामारी की तरह अपने पैर पसार रही है। समाजकार्य लगातार समाज में पनपने वाली समस्याओं के खिलाफ किये जाने वाले सकारात्मक प्रयासो में पहली पंक्ति में खड़ा रहा है, जिसका कारण समाजकार्य का समाज से सबसे निकट व घनिष्ठ संबंध होना रहा है। इस कारण समाजकार्य का महत्वपूर्ण हस्तक्षेप समाज की समस्याओं को निपटाने के संबंध में रहा है, क्योंकि उनका मुख्य उद्देश्य समाज के विभिन्न हिस्सों को समर्थन देना और उनके जीवन स्तर को सुधारना है। समाजकार्य का हस्तक्षेप साइबर अपराध की रोकथाम, जागरूकता और पीड़ितों को सहायता प्रदान करने में प्रभावी हो सकता है। बहरहाल सामान्यतः सामाजिक कार्यकर्ताओं का साइबर क्राइम के क्षेत्र में प्रशिक्षण, शिक्षण व अनुभव का अभाव है जिसे पूर्ण किए जाने की आवश्यकता है परंतु बहुत से ऐसे सामाजिक कार्यकर्ता हैं जो इन मामलों में प्रशिक्षित हैं और साइबर क्राइम की रोकथाम में महत्वपूर्ण भूमिका में हैं। हालांकि साइबर सुरक्षा के प्रति आम जन-मानस को जागरूक करने, उन्हे सतर्क करने तथा डिजिटल प्लेटफार्म के सकारात्मक उपयोग करने हेतु प्रशिक्षित किए जाने की अत्यंत आवश्यकता है। जिसके तहत सामाजिक कार्य पेशेवरों के माध्यम से साइबर सुरक्षा और जागरूकता कार्यक्रमों का संचालन किया जाता है। समाजकार्य पेशेवरों द्वारा साइबर सुरक्षा और इंटरनेट की सुरक्षित उपयोगिता पर जागरूकता कार्यक्रम चलाए जा सकते हैं। इससे लोग साइबर अपराधों के प्रति सजग होंगे और यह समझेंगे कि वे किस प्रकार अपनी व्यक्तिगत जानकारी की सुरक्षा कर सकते हैं। सामाजिक कार्य के तहत हस्तक्षेप द्वारा स्कूलों, कॉलेजों और समुदायों में साइबर सुरक्षा पर कार्यशालाओं का आयोजन किया जाता है जिससे लोगों को इंटरनेट और सोशल मीडिया के सुरक्षित उपयोग के बारे में मार्गदर्शन दिया जा सके। साइबर बुलीइंग एक गंभीर समस्या है जो किसी भी सामाजिक प्राणी के मानसिक स्वास्थ्य को प्रभावित कर सकती है। समाजकार्य पेशेवर इस क्षेत्र में हस्तक्षेप कर सकतें हैं, पीड़ितों को मानसिक और भावनात्मक समर्थन प्रदान कर सकते हैं और साइबर बुलीइंग से निपटने के लिए उन्हें मनोवैज्ञानिक सलाह दे सकते हैं। साइबर बुलीइंग से प्रभावित बच्चों और युवाओं के लिए काउंसलिंग और मानसिक स्वास्थ्य सेवाएं उन्हे उनकी हद व पहुँच मे उपलब्ध करवाने में समाजकार्य पेशेवर का हस्तक्षेप जरूरी है। पीड़ितों को उनके अधिकारों और उपलब्ध सहायता संसाधनों के बारे में जानकारी देना, सुविधाओं तक उनकी पहुँच सुनिश्चित करना, समाजकार्य पेशेवर का दायित्व बन जाता है। समाजकार्य पेशेवर के हस्तक्षेप द्वारा साइबर अपराध के शिकार लोगों को उचित कानूनी सहायता और मार्गदर्शन की आवश्यकता की पूर्ति की जाती है। समाजकार्य पेशेवर इन लोगों को सहायता प्रदान कर सकते हैं, उन्हें उनके अधिकारों के बारे में अवगत करवाते हैं, और जरूरत पड़ने पर कानूनी कार्रवाई के लिए उपयुक्त अधिकारियों से संपर्क करने में मदद कर सकते हैं। समाजकार्य पेशेवर द्वारा समय- समय पर पीड़ितों को कानूनी सहायता और उनके अधिकारों के बारे में जानकारी प्रदान करना। साइबर अपराधों के मामलों में काउंसलिंग और सामाजिक सहायता प्रदान करना। समाजकार्य पेशेवर समुदाय स्तर पर हस्तक्षेप करते हैं, जहाँ वे समुदाय के सदस्यों को साइबर अपराधों के खतरों से अवगत कराते हैं और एक सकारात्मक, सहयोगी और सुरक्षित साइबर वातावरण बनाने के लिए समुदाय के विभिन्न हिस्सों को एकजुट करते हैं। समुदायों के साथ मिलकर साइबर अपराधों की रोकथाम के लिए कार्यक्रम आयोजित करना। समाज के विभिन्न हिस्सों को एकजुट कर साइबर सुरक्षा से संबंधित पहलुओं पर चर्चा करना। समाजकार्य पेशेवर विभिन्न सरकारी और गैर-सरकारी संगठनों, पुलिस, और अन्य कानून प्रवर्तन एजेंसियों के साथ मिलकर साइबर अपराध की रोकथाम में मदद करते हैं। वे एक नेटवर्क बनाते हैं जो विभिन्न पक्षों को जोड़कर सामूहिक प्रयास कर सके। साइबर अपराध की रोकथाम के लिए विभिन्न संगठनों और संस्थाओं के साथ सहयोग और नेटवर्किंग लोगों को साइबर अपराधों के बारे में रिपोर्ट करने के लिए प्रोत्साहित करना तथा उन मामलों की निगरानी रखना समाजकार्य पेशेवर कार्यकर्ताओं की पहल से सकारात्मक प्रभाव डालती है। समाजकार्य पेशेवर अपराधियों के पुनर्वास और सुधार में भी मदद करते हैं। वे उन व्यक्तियों को सामाजिक और मानसिक सहायता प्रदान

कर सकते हैं, जो साइबर अपराधों में लिप्त हो चुके हैं, ताकि वे भविष्य में पुनः अपराध न करें। साइबर अपराधियों के लिए सुधारात्मक कार्यक्रम और काउंसलिंग सत्र आयोजित करना तथा उन्हे समायोजन के लिए प्रोत्साहित करना, अपराधियों को समाज में फिर से समाहित करने का प्रयास व उन्हे पुनः नियोजन का मौका देना। समाजकार्य पेशेवरों का प्रमुख उद्देश्य समाज में सुधार लाना और उन लोगों को सहायता प्रदान करना है, जिन्हें विभिन्न प्रकार की समस्याओं का सामना करना पड़ रहा है। साइबर अपराधों की बढ़ती संख्या ने समाज कार्य पेशेवरों के लिए एक नया क्षेत्र प्रस्तुत किया है, जहां वे न केवल पीड़ितों को सहायता प्रदान कर सकते हैं, बल्कि समाज में जागरूकता फैलाने और इस समस्या की जड़ तक पहुंचने में भी मदद कर सकते हैं। समाज कार्य पेशेवरों का मुख्य उद्देश्य समाज में समस्याओं का समाधान करना और पीड़ितों को समर्थन देना होता है। साइबर अपराध एक गंभीर सामाजिक समस्या है, जिसके प्रभाव समाज के विभिन्न वर्गों पर पड़ते हैं, विशेष रूप से बच्चों, युवाओं, महिलाओं, और वरिष्ठ नागरिकों पर। समाजकार्य पेशेवरों का इस क्षेत्र में महत्वपूर्ण योगदान है। साइबर अपराध के शिकार लोगों को अक्सर मानसिक और भावनात्मक आघात का सामना करना पड़ता है। समाजकार्य पेशेवर लोगों को सामाजिक रूपों से की गयी साइबर बुलीइंग, फिशिंग, ऑनलाइन धोखाधड़ी, और अन्य साइबर अपराधों के शिकार लोगों की काउंसलिंग और मानसिक सबलता प्रदान कर सकते हैं। सकारात्मक काउंसलिंग की मदद से पीड़ित व्यक्ति को अपना मानसिक स्वास्थ्य पुनः प्राप्त करने में मदद मिलती है, जो लोगों को अपराध के प्रभावों से उबरने में सक्षम बनाता है। समाजकार्य पेशेवरों द्वारा समुदायों, स्कूलों और अन्य संस्थानों में साइबर सुरक्षा पर जागरूकता अभियान चलाए जाते हैं। इससे लोगों को यह समझने में मदद मिलती है कि वे अपने व्यक्तिगत डेटा की सुरक्षा कैसे कर सकते हैं और साइबर अपराधों से बचने के लिए क्या कदम उठा सकते हैं। ये कार्यक्रम विशेष रूप से बच्चों और युवाओं को साइबर अपराधों से बचने के लिए जरूरी जानकारी व प्रशिक्षण मे सहयोगी होतें है जैसे कि सोशल मीडिया पर सुरक्षित तरीके से बातचीत करना और अनजान लिंक से बचना। काउंसिलिंग की मदद से व्यक्ति की मानसिक और भावनात्मक स्थिति को स्थायित्व प्रदान किया जा सकता हैं। जागरूकता कार्यक्रम समाज के विभिन्न वर्गों के लिए विशेष रूप से डिज़ाइन किए जा रहें हैं, जैसे कि बुजुर्गों, महिलाओं, और बच्चों के लिए, ताकि वे साइबर अपराधों से सुरक्षित रह सकें। वे समाज के भीतर एक सहयोगी और सुरक्षित डिजिटल वातावरण बनाने के लिए काम करते हैं, ताकि लोगों में आपसी विश्वास और सहयोग बढ़े। साइबर अपराध की बढ़ती संख्या ने न केवल कानूनी और तकनीकी क्षेत्रों को चुनौती दी है, बल्कि समाज में गहरी मानसिक और सामाजिक समस्याएँ भी उत्पन्न की हैं जिनकी संख्या तेजी से बढ़ रही है। समाज के विभिन्न हिस्सों को समर्पित और समग्र सहायता प्रदान करने वालें पेशेवर समाज कार्यकर्ता साइबर अपराध की रोकथाम और प्रभावी हस्तक्षेप में एक सक्रिय भूमिका निभा सकते हैं, जो सामाजिक बदलाव, जागरूकता और समर्थन के विभिन्न पहलुओं पर आधारित हो। पेशेवर समाज कार्यकर्ता द्वारा सेवार्थी को कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT) और पुलिस से संपर्क, सहायता और समन्वय स्थापित। "कंप्यूटर", "डिजिटल सिग्नेचर", "इलेक्ट्रॉनिक रिकॉर्ड", "साइबर अपराध" इलेक्ट्रॉनिक रिकॉर्ड की वैधता आदि का ज्ञान जन-जन तक पहुचाना पेशेवर समाज कार्यकर्ता की नैतिक ज़िम्मेदारी बन जाती है।

निष्कर्ष-

साइबर अपराध की रोकथाम में पेशेवर समाजकार्य का हस्तक्षेप न केवल पीड़ितों को मानसिक, भावनात्मक और कानूनी सहायता प्रदान करने तक सीमित है, बल्कि यह समुदाय और साइबर अपराधियों के सुधार के लिए भी कार्य करता है। समाज कार्य पेशेवर साइबर अपराधों के प्रति जागरूकता फैलाने, लोगों को सुरक्षित डिजिटल व्यवहार के लिए प्रशिक्षित करने, और साइबर अपराधियों के लिए पुनर्वास कार्यक्रमों की स्थापना में सक्रिय भूमिका निभाते हैं। उनका योगदान साइबर अपराधों की रोकथाम में सामाजिक, कानूनी और मानसिक दृष्टिकोण से महत्वपूर्ण हो सकता है। साइबर अपराध और समाज कार्य का संबंध समाज की समृद्धि और सुरक्षा से जुड़ा हुआ है। समाजकार्य पेशेवर इस क्षेत्र में महत्वपूर्ण भूमिका निभा सकते हैं, न केवल साइबर अपराधों की रोकथाम में, बल्कि पीड़ितों को सहायता, कानूनी मार्गदर्शन, और मानसिक स्वास्थ्य समर्थन भी प्रदान कर सकते हैं। साथ ही, समाजकार्य पेशेवर समाज में जागरूकता फैलाकर और सुरक्षा उपायों को बढ़ावा देकर साइबर अपराध की बढ़ती हुई समस्या को कम करने में योगदान कर सकते हैं। समाजकार्य पेशेवरों का साइबर अपराध की रोकथाम में महत्वपूर्ण हस्तक्षेप हो सकता है, क्योंकि वे न केवल पीड़ितों को सहायता प्रदान करते हैं, बल्कि अपराधियों के सुधार, समाज में जागरूकता फैलाने, और समुदायों को साइबर सुरक्षा के महत्व के बारे में अवगत करने में भी महत्वपूर्ण भूमिका निभा सकते हैं। इसके अतिरिक्त, समाजकार्य पेशेवरों के पास पीड़ितों के मानसिक और भावनात्मक समर्थन का कौशल होता है, जो साइबर अपराधों के प्रभावों से उबरने में महत्वपूर्ण है।Information Technology Act, 2000** भारत में डिजिटल दुनिया के लिए एक महत्वपूर्ण कानूनी ढांचा है। यह न केवल ई-व्यवसाय, इलेक्ट्रॉनिक रिकॉर्ड और डिजिटल दस्तावेजों की

वैधता को सुनिश्चित करता है, बल्कि साइबर अपराधों को नियंत्रित करने के लिए एक मजबूत कानूनी प्रणाली भी प्रदान करता है। इस एक्ट के माध्यम से साइबर अपराधियों के खिलाफ कार्रवाई की जाती है, और नागरिकों की ऑनलाइन सुरक्षा सुनिश्चित की जाती है। नागरिकों को चाहिए की वे अनजानी ईमेल या लिंक पर क्लिक करने से बचें। अपनी व्यक्तिगत जानकारी को ऑनलाइन साझा करते वक्त सतर्क रहें। एंटीवायरस सॉफ़्टवेयर का उपयोग करें और उसे अपडेट रखें। सार्वजनिक वाई-फाई नेटवर्क पर संवेदनशील जानकारी का आदान-प्रदान न करें। जिससे साइबर अपराधियों तक उनकी पहुच को कम किया जा सके।

संदर्भ-

https://cybervolunteer.mha.gov.in/
https://www.fbi.gov/investigate/cyber
https://mhcyber.gov.in/report-complaint
https://cyberpolice.nic.in/
https://www.interpol.int/en/Crimes/Cybercrime
https://hi.wikipedia.org/wiki/%E0%A4%B8%E0%A4%BE%E0%A4%88%E0%A4%AC%E0%A4%B0_%E0%A4%85%E0%A4%AA%E0%A4%B0%E0%A4%BE%E0%A4%A7
https://readerblogs.navbharattimes.indiatimes.com/animeshsharma/cyber-security-issues-current-indian-cyber-laws-and-steps-to-be-taken/
https://incometaxindia.gov.in/hindi/pages/acts/information-technology-act.aspx
https://egovernance.vikaspedia.in/viewcontent/e-governance/about-rti-act-2005/93894291a92893e
https://indiankanoon.org/doc/1965344/
https://एमईआईटीवाई.सरकार.भारत/writereaddata/files/DG-CERT-RR-notification%281%29_0.pdf
https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2068522
https://prsindia.org/theprsblog/a-background-to-section-66a-of-the-it-act-2000?page=2&per-page=1
https://www.scobserver.in/cases/peoples-union-for-civil-liberties-implementation-of-s-66a-it-act-case-background/
https://www.bbc.com/hindi/india-63238374
https://services.india.gov.in/service/detail/%E0%A4%B8%E0%A5%82%E0%A4%9A%E0%A4%A8%E0%A4%BE
https://www.indiacode.nic.in/handle/123456789/1999
Information Technology Act, 2000 (IT Act, 2018)
https://infosecawareness.in/cyber-laws-of-india
https://www.axiomlaw.com/guides/cyber-law
https://www.bhaskar.com/news/cybercrime-from-fines-to-it-act-to-life-in-prison-041519-3011019.html
https://cybercrime.gov.in/
https://services.india.gov.in/service/detail/national-cyber-crime-reporting-portal
https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime
https://cytrain.ncrb.gov.in/