Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0052

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

सायबर क्राईम आणि व्यावसायीक समाजकार्य आव्हाने आणि मध्यस्थीचे उपाय

सहा. प्रा. कु. रंजना एच. आडे
जोतीराव फुले समाजकार्य
महाविद्यालय उमरेड, जि. नागपूर
Email :-rajaniade08@gmail.com
Mo :- 9764579834

प्रस्तावना:

सायबर क्राईम म्हणजे संगणक इंटरनेट, मोबाईल आणि डिजिटल तंत्रज्ञानाचा गैरवापर करून केलेले गुन्हे, या गुन्ह्यांमध्ये डेटा चोरी, फसवणूक, हॅकिंग, ऑनलाईन गैरवर्तन, आणि आर्थिक फसवणूक यांचा समावेश होतो, हे गुन्हे वैयक्तिक, सामाजिक, आणि आर्थिक नुकसान घडवून आणतात, तंत्रज्ञानाच्या प्रगतीमूळे आपले जिवन सुलभ असले तरी त्याच वेळी सायबर गुन्ह्यांचे प्रमाण मोठ्य प्रमाणात वाढले आहेत, इंटरनेट, सोशल मीडिया, ऑनलाईन व्यवहार आणि डिजिटल संवादाच्या वाढत्या वापरामुळे गुन्हेगारांना नवीन संधी उपलब्ध झाल्या आहेत.

सायबर क्राईम ही केवळ तांत्रिक किंवा कायदेशीर समस्या नाही, तर ती सामाजिक समस्या देखील आहे. व्यावसायिक समाजकार्य (Professional social work) यामध्ये मानसिक आरोग्य समुपदेशन जनजागृती आणि पुनर्वसन या सारख्या क्षेत्रांमध्ये योगदान देऊ शकते.

सायबर क्राईम प्रकार (Types of cyber crime)

१) ऑनलाईन फसवणूक:– (Fraud)

ऑनलाईन फसवणूक म्हणजे इंटरनेटच्या माध्यामातून लोकांची फसवणूक करून त्यांच्या कडून पैसे, वैयक्तिक माहिती किंवा इतर संवेदनशील डेटा चोरी करणे, डिजिटल तंत्रज्ञानाच्या वाढत्या वापरामुळे अशा फसवणुकीचे प्रमाण झपाट्याने वाढत आहे.

२) हॅकिंग आणि डेटा चोरी:–

हॅकिंग म्हणजे अनाधिकृतरित्या संगणक प्रणाली, नेटवर्क किंवा डिजिटल उपकरणांमध्ये प्रवेश करून माहिती चोरणे, बदल करणे, किंवा त्याचा गैरवापर करणे. हॅकिंगचा वापर व्यक्तिगत, आर्थिक आणि व्यावसायिक माहिती चोरीसाठी केला जातो.

डेटा चोरी म्हणजे कोणत्याही व्यक्ति, संस्था किंवा सरकारच्या परवानगीशिवाय संवेदनशील माहिती मिळवणे आणि तिचा गैरवापर करणे.

३) सोशल मीडिया गैरवापर:– (Social Media Exploitation)

सोशल मेडिया हे संवाद, माहिती आदान प्रदान आणी सामाजिक जाळे निर्माण करण्याचे प्रभावी साधन आहे. मात्र याचा गैरवापर केल्यामुळे वैयक्तिक, सामाजिक आणि राष्ट्रीय पातळीवर अनेक गंभीर परिणाम दिसून येतात.

४) सायबर बुलींग आणि ट्रोलींग:– (Cyber Bullying & Trolling)

डिजिटल जगाच्या वाढत्या प्रभावामुळे सायबर बुलींग आणि ट्रोलींग ही मोठी सामाजिक समस्या बनली आहे. इंटरनेट आणि सोशल मीडियाच्या माध्यामातून एखाद्या व्यक्तीला मानसिक त्रास देणे, धमक्या देणे, किंवा बदनामी करणे म्हणजे सायबर बुलींग, ट्रोलींग म्हणजे सोशल मिडियावर जाणीवपूर्वक वाद निर्माण करणे, व्देषात्मक, आक्षेपार्ह कमेंट्स करणे.

५) डिजिटल लैंगिक शोषण :– (Cyber Harassment & Exploitation)

डिजिटल तंत्रज्ञानाच्या वाढत्या वापरामुळे लैंगिक शोषणाचे स्वरुप ही ऑनलाइन माध्यमातून बदलले आहे. इंटरनेट आणि सोशल मीडियाचा गैरवापर करून महिलांना मुलींना वेगवेगळ्या प्रकारे त्रास दिला जातो, यामध्ये ब्लॅकमेलिंग, अश्लील फोटो/व्हिडिओचा गैरवापर ऑनलाईन गंडा, मॉर्फींग रिव्हेंज पोर्न आणि सेक्स्टॉर्शन यांसारख्या घटना घडतात.

६) फिशिंग आणि मालवेअर हल्ले:– (Phishing & Malware Attacks)

डिजिटल जगात सायबर सुरक्षेला सर्वात मोठा धोका म्हणजे फिशिंग आणि मालवेअर हल्ले हे सायबर गुन्हेगारांकडून वैयक्तिक, वित्तीय, किंवा गोपनीय माहिती चोरण्यासाठी आणि संगणक प्रणालीमध्ये अनधिकृत प्रवेश मिळवण्यासाठी केले जातात.

१) फिशिंग म्हणजे काय :– फिशिंग हा सायबर गुन्हेगारांकडून केला जाणारा फसवणुकीचा प्रकार आहे. ज्यामध्ये लोकांना बनावट ई–मेल, मेसेज किंवा वेबसाईटच्या माध्यामातून फसवून त्यांची गोपनीय माहिती उकळली जाते. यामध्ये बँक खात्याची माहिती, पासवर्ड, क्रेडिट कार्ड डिटेल्स, आधार किंवा पॅन क्रमांक अशा संवेदनशील गोष्टींचा समावेश असतो.

फिशिंगचे प्रकार:–

१) ई–मेल फिशिंग:– बनावट बँक किंवा कंपनीच्या नावाने ई–मेल पाठवले जातात, यामध्ये तुमचे खाते ब्लॉक झाले आहे, तुम्हाला मोठी लॉटरी लागली आहे असे भ्रामक संदेश असतात, यातील लिंकवर क्लिक केल्यास तुम्हाला बनावट वेबसाईटवर नेले जाते, आणि तुमची माहीती चोरण्यात येते.

२) एस.एम.एस. फिशिंग:– तुमच्या खात्याची KYC अपडेट करा संदर्भात मेसेज असतात.

३) व्हाईस फिशिंग:– बँकेच्या किंवा सरकारी अधिकाऱ्याच्या नावाने कॉल करुन OTP, डेबिट कार्ड नंबर किंवा पिन विचारला जातो.

४) स्पिअर फिशिंग:– विशिष्ट व्यक्ति किंवा कंपनीला लक्ष्म करून फिशिंग ई–मेल पाठवले जातात, हे प्रामुख्याने कॉर्पोरेट कंपन्या आणि सरकारी संस्थामध्ये डेटा चोरण्यासाठी वापरले जाते.

सायबर क्राईमचे सामाजिक परिणाम (Social Impact of Cyber Crime)

१) मानसिक तणाव आणि नैराश्य
२) कौटुंबिक आणि सामाजिक नाती प्रभावित होणे
३) आर्थिक नुकसान
४) महिला, मूल, वृद्ध, यांच्यावर होणारा विशेष प्रभाव.

व्यावसायिक समाजकार्याची भूमिका:–

१) प्रतिबंधात्मक उपाय:– १) जनजागृती आणि सायबर सुरक्षा शिक्षण.
२) शाळा, महाविद्यालये आणि समुदायात कार्यशाळा.

२) सायको सोशल सपोर्ट:–१) सायबर क्राईमच्या शिकार झालेल्या समुपदेशन आणि मानसिक आधार.
२) क्रायसेस इंटरव्हेन्शन मॉडेलचा वापर.

३) पॉलिसी ॲडव्होकेसी:– १) सरकार, कायदयाच्या यंत्रणा आणि सामाजिक संस्थांशी समन्वय.
२) सायबर क्राईम प्रतिबंधक धोरणात सामाजिक दृष्टीकोनाचा समावेश.

४) कौटुंबिक आणि सामाजिक पूर्नवसन:– १) सायबर गुन्ह्यांमध्ये अडकलेल्या व्यक्तींना पुन्हा समाजात सामावून घेण्यासाठी उपाययोजना
२) शैक्षणिक आणि व्यावसायिक मार्गदर्शन

सायबर क्राईमचे मुख्य प्रकार

१) व्यक्तिगत सायबर गुन्हे:–

१) सायबर बुलींग व्दारे सोशल मीडियावर धमक्या देणे, ट्रोलींग करणे.
२) सायबर स्टॉकींग व्दारे ऑनलाईन पाठलाग आणि छळ.
३) फसवणूक आणि चोरी याद्वारे वैयक्तीक माहिती चोरणे.

२) आर्थिक सायबर गुन्हे:–

फिशिंग फेक ई–मेल किंवा वेबसाइटद्वारे बँक माहिती चोरणे, ऑनलाईन फसवणूक, बनावट लॉटरी, इन्व्हेस्टमेंट स्कीम, क्रेडिट कार्ड फ्रॉड कार्डाची माहिती हॅक करून पैसे काढणे.

३) संस्थात्मक सायबर गुन्हे:–

१) हॅकिंग :– सरकारी किंवा खासगी संस्थांच्या डेटा सेंटरमध्ये अनाधिकृत प्रवेश
२) डेटा ब्रीच:– संवेदनशील माहिती लीक करणे

३)मालवेअर आणि व्हायरस हल्ले:–

सॉफ्टवेअर किंवा सिस्टम डॅमेज करणे

४) सामाजिक आणि नैतिक सायबर गुन्हे:–

सोशल मीडिया गैरवापर– खोटी माहिती आणि अफवा पसरवणे
डिजिटल मानहानी– कुणाच्या प्रतिष्ठेचे नुकसान करणे
बालशोषण आणि पोर्नोग्राफी– अवैध डिजिटल सामग्रीचे वितरण

सायबर क्राईमचे परिणाम:–

१) मानसीक तणाव आणि आत्महत्येच्या घटना
२) आर्थिक नुकसान
३) सामाजिक प्रतिष्ठेचे नुकसान
४) वैयक्तिक आणि कौटुंबिक संबंधावर परिणाम

सायबर क्राईम प्रतिबंधक उपाय:–

१) मजबूत पासवर्ड आणि डिजिटल सुरक्षा प्रणालीचा वापर
२) विश्वसनीय वेबसाइट, आणि लिंक क्लिक करण्याचे टाळणे
३) सायबर कायद्यांची माहिती आणि सतर्कता

४) सायबर सुरक्षा उपाय शिकविण्यासाठी शाळा महाविद्यालये आणि समाजात जागरूकता अभियान भारतात माहिती तंत्रज्ञान कायदा २००० (IT Act, २०००) अंतर्गत सायबर क्राईम विरोधात कारवाई केली जाते, व्यावसायिक समाजकार्य यात प्रभावी भूमिका बजावू शकते, जसे की जनजागृती, समुपदेशन, आणि कायदेशीर मदत पुरवणे.

डिजिटल तंत्रज्ञानाच्या वाढत्या वापरामुळे सायबर गुन्ह्यांमध्ये झालेली वाढ:–

तंत्रज्ञानाच्या प्रगतीमुळे आपले जिवन सुलभ झाले असले तरी त्याच वेळी सायबर गुन्ह्यांमध्ये फार मोठ्या प्रमाणात वाढझालेली आहे. इंटरनेट, सोशल मीडिया ऑनलाईन व्यवहार, डिजिटल संवादाच्या वापरामुळे गुन्हेगारांना संधी उपलब्ध झाल्या.

डिजिटल तंत्रज्ञानाच्या वाढत्या वापरामुळे सायबर गुन्ह्यांमध्ये वाढ होण्याची कारणे

१) इंटरनेट आणि मोबाईलच्या सर्वसामान्य वापरात वाढ:–

इंटरनेट आणि स्मार्टफोनच्या सहज उपलब्धतेमुळे लोक मोठ्या प्रमाणावर ऑनलाईन व्यवहार करू लागले आहेत. ग्रामीण भागातही डिजिटल सेवा वाढल्याने इंटरनेट वापरकर्त्यांची संख्या झपाट्याने वाढत आहे.

२) ऑनलाइन आर्थिक व्यवहार आणि डिजिटल पेमेंट सिस्टम:–

ऑनलाइन बँकिंग, डिजिटल वॉलेट, (UPI, Paytm, Google Pay) यांच्या मोठ्या प्रमाणावर वापर होतो. यामुळे फिशिंग OTP फ्रॉड आणि कार्ड क्लोनिंग सारख्या आर्थिक फसवणुकीत वाढझाली आहे.

३) सोशल मीडिया आणि माहिती शेअरिंगचा वाढता प्रमाण:–

लोक सहजरीत्या आपली वैयक्तिक माहिती सोशल मीडियावर शेअर करतात. खोटी ओळख निर्माण करून फसवणूक करणाऱ्या गुन्हेगारांसाठी ही माहिती महत्त्वाची ठरते. फेक न्यूज, ट्रोलींग आणि सोशल मीडियाद्वारे गैरवर्तन वाढले आहे.

४) डेटा चोरी आणि हॅकिंगच्या घटना:–

मोठ्या प्रमाणावर सरकारी आणि खाजगी संस्थांचा डेटा ऑनलाइन स्टोर केला जातो. सायबर गुन्हेगार हॅकिंग द्वारे ही संवेदनशील माहिती चोरून चुकीच्या पद्धतीने वापरतात.

५) कृत्रिम बुद्धिमत्ता(AI)आणि डीपफेक(Deep Fake) तंत्रज्ञानाचा वापर:–

AIआणि डीपफेक तंत्रज्ञानाचा वापर करून खोट्या व्हिडिओ आणि ऑडिओ क्लिप तयार केल्या जातात. याचा वापर चुकीची माहिती पसरवण्यासाठी किंवा ब्लॅकमेल करण्यासाठी केला जातो.

सायबर गुन्ह्यांमध्ये झालेली वाढ: आकडेवारी आणि उदाहरणे

१) NCRB (National Crime Records Bureau) च्या अहवालानुसार भारतात सायबर गुन्ह्यांचे प्रमाण दरवर्षी २०–२५ टक्के ने वाढत आहे.
२) २०१९ मध्ये ४४,५४६ सायबर गुन्हे नोंदवले आहे. तर २०२१ मध्ये तेज प्रमाण ५०,०३४ वर गेले आहे.
३) ऑनलाइन आर्थिक फसवणुकीची प्रकरणे विशेषत: लहान शहरांमध्ये वाढत आहेत.

सायबर गुन्हे रोखण्यासाठी उपाय योजना :–

१) वैयक्तिक उपाय:–

मजबूत पासवर्ड आणि दोन स्तरीय सुरक्षा वापरणे, अनाधिकृत आणि अविश्वसनीय वेबसाईटवर माहिती न भरता सतर्क राहणे. सोशल मीडियावर वैयक्तिक माहिती जास्त शेअर न करणे.

२) शैक्षणिक आणि संस्थात्मक उपाय:–

शाळा, महाविद्यालये आणि कार्यशाळांमध्ये सायबर सुरक्षा शिक्षण अनिवार्य करणे. कंपन्यांनी आणि सरकारी संस्थांनी सायबर सुरक्षा प्रणाली अधिक मजबूत करणे.

३) कायदेशीर उपाय:–

माहिती तंत्रज्ञान कायदा २०००(IT Act, २०००) च्या कठोर अंमलबजावणीसाठी सरकारने कठोर उपाय योजना करणे. सायबर गुन्हे रोखण्यासाठी विशेष पोलीस पथके आणि सायबर हेल्पलाइन सुरू करणे.

समाजकार्य व्यवसायाचा सायबर क्राईम मध्ये हस्तक्षेप करण्याचा संभाव्य दृष्टिकोन:–

सायबर क्राईम ही केवळ तांत्रिक किंवा कायदेशीर समस्या नाही तर ती सामाजिक समस्या देखील आहे. व्यावसायिक समाजकार्य यामध्ये मानसिक, आरोग्य, समुपदेशन, जनजागृती आणि पुनर्वसन यासारख्या क्षेत्रांमध्ये योगदान देऊ शकते.

१) प्रतिबंधात्मक उपाय:–

समाजकार्याचा मुख्य उद्देश समाजामध्ये सायबर सुरक्षा आणि जबाबदारी बाबत जनजागृती करणे आहे.

१) शाळा आणि महाविद्यालयांमध्ये सायबर सुरक्षा शिक्षण देणे.
२) सायबर क्राईम बाबत कार्यशाळा आणि मोहीम राबवणे.
३) सामाजिक माध्यमांचा जबाबदारीने वापर करण्यासाठी मार्गदर्शन करणे.

२) सायको सोशल सपोर्ट:–

सायबर गुन्ह्यांचा बळी ठरलेल्या व्यक्तींवर मोठा मानसिक आणि सामाजिक परिणाम होतो.

१) सायबर बॉलिंग, ट्रोलिंग आणि सोशल मीडियावर बदनामीच्या घटनांमध्ये समुपदेशन करणे.

२) सायबर गुन्ह्यांमुळे मानसिक तणाव आणि नैराश्य आलेल्या व्यक्तींना आधार देणे.

३) वैयक्तिक आणि कौटुंबिक समुपदेशनाद्वारे सायबर गुन्ह्यांचे परिणाम कमी करण्यासाठी मदत करणे.

३) कायदेशीर आणि धोरणात्मक हस्तक्षेप:–

१) सायबर सुरक्षा कायद्यांबाबत जनजागृती करणे.

२) सायबर गुन्ह्यांची शिकार झालेल्या लोकांना पोलिस आणि कायदेशीर मदत मिळवून देणे.

३) सरकार आणि न्याय संस्थेबरोबर काम करून अधिक प्रभावी धोरणे राबविण्यात मदत करणे.

४) पुनर्वसन आणि समाजामध्ये पुनर्स्थापन:–

१) सायबर गुन्ह्यांमध्ये अडकलेल्या युवकांना मुख्य प्रवाहात आणण्यासाठी पुनर्वसन केंद्र चालविणे.

२) सायबर गुन्हेगारांना शिक्षणाने समुपदेशनाच्या माध्यमातून सुधारण्यासाठी उपाययोजना करणे.

३) सायबर गुन्ह्यांचे बळी ठरलेल्या व्यक्तींना समाजामध्ये पुनर स्थापित करण्यासाठी सहकार्य करणे.

५) कायदेशीर उपाय:–

भारत सरकारने सायबर सुरक्षेसाठी काही कायदे लागू केले आहेत.

१) IT Act 2000फिशिंग आणि मालवेअर हल्ल्यांविरुद्ध कठोर शिक्षा

२) IPC 420फसवणुकीसाठी शिक्षा

३) IPC 379डेटा चोरीसाठी शिक्षा

४) सायबर क्राईम हेल्पलाइन १९३०

५) सायबर क्राईम पोर्टल www.cybercrime.gov.in

संदर्भ ग्रंथ

१) सायबर धोके आणि उपाय योजना – डॉ. दीपक शिकारपूर