IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

साइबर अपराध एक सामाजिक एवं मनोवैज्ञानिक समस्याः एक विश्लेषणात्मक अध्ययन।

प्रतिभा यादव

शोध छात्रा, शिक्षाशास्त्र, जीवाजी विश्वविद्यालय ग्वालियर, म.प्र.

डॉ. नितिन बाजपेयी

सहायक प्रोफेसर, बी.एड. विभाग, महाराणा प्रताप राजकीय स्नातकोत्तर महाविद्यालय हरदोई।

सारांश –आज के डिजिटल युग में तकनीकी प्रगति ने जहां हमारे जीवन को आसान बनाया है वहीं इसके दुष्परिणाम भी सामने आने लगे हैं इन्हीं में से एक है साइबर अपराध, जो समाज के लिए गंभीर चुनौती है। साइबर अपराध में तकनीकी का सहारा लिया जाता है लेकिन इसका संबंध केवल तकनीकी ज्ञान से नहीं है, बल्कि अपराधियों की सामाजिक स्थिति एवं उनकी मानसिकता और पीड़ितों की मनोवैज्ञानिक स्थिति से भी होता है, साइबर अपराध तकनीकी प्रगति के साथ एक गंभीर सामाजिक समस्या भी बन गयी है। यह अपराध केवल तकनीकी पहलुओं तक सीमित नहीं है बल्कि इसके पीछे अपराधियों की सामाजिक स्थिति एवं मनोवैज्ञानिक प्रवृत्तियां भी महत्वपूर्ण भूमिका निभाती हैं यह शोध पत्र साइबर अपराध के सामाजिक एवं मनोवैज्ञानिक पहलुओं का विश्लेषण करता है जिसमें अपराधियों की सामाजिक स्थितियां एवं उनकी मानसिकता, उनकी प्रेरणाएँ और पीड़ितों पर पड़ने वाले सामाजिक और मानसिक प्रभाव शामिल हैं साइबर अपराधी विभिन्न सामाजिक और मनोवैज्ञानिक कारणों से अपराध करते हैं जैसे– बेरोजगारी, आर्थिक लालच, शक्ति की इच्छा, मनोरोगी प्रवृत्तियां, डिजिटल साक्षरता की कमी, सामाजिक असमानता एवं प्रतिशोध, सामाजिक अलगाव, जोखिम लेने की प्रवृत्ति, सोशल मीडिया का प्रभाव, समाज की उदासीनता, साइबर अपराध का आसान और कम खर्चीला स्वरूप, अपराधी की मानसिक विकृति, डिजिटल नशा और इंटरनेट की लत आदि। इन अपराधों के कारण पीड़ितों में चिंता, अवसाद, आत्मसम्मान में कमी, आत्महानि, पारिवारिक और सामाजिक रिश्तों में दरार, समाज में अविश्वास और डर का माहौल, सामाजिक शर्मिंदगी, अपराध बोध, डिजिटल फोबिया और पोस्ट– ट्रामेटिक स्ट्रेस डिसऑर्डर जैसे मानसिक विकार देखे जाते हैं। प्रस्तुत शोध पत्र में विभिन्न प्रकार के साइबर अपराधों पर चर्चा की गई है साथ ही साइबर अपराध को रोकने के लिए सामाजिक और मनोवैज्ञानिक उपायों जैसे – साइबर जागरूकता, डिजिटल नैतिकता, काउंसलिंग, सामुदायिक सहभागिता, संज्ञानात्मक व्यवहार तकनीकी, मानसिक स्वास्थ्य सहायता, मनोविकार प्रवृत्ति और साइबर सुरक्षा प्रशिक्षण पर प्रकाश डाला गया है। प्रस्तुत शोध पत्र का उद्देश्य साइबर अपराध को केवल तकनीकि समस्या न मानकर इसे एक मनोवैज्ञानिक और सामाजिक समस्या के रूप में भी समझना चाहिए , इसका विश्लेषण करना है। अपराधियों की सामाजिक स्थिति और मानसिकता और पीड़ितों के मनोवैज्ञानिक स्थिति को समझकर इस समस्या का प्रभावी समाधान खोजा जा सकता है।

मुख्य शब्द : साइबर अपराध, साइबर सुरक्षा, सामाजिक–मनोवैज्ञानिक पहलू, साइबर मनोविज्ञान, साइबर जागरूकता

प्रस्तावनाः साइबर क्राइम उन अपराधों को कहते हैं जो इंटरनेट, कंप्यूटर सिस्टम, मोबाइल डिवाइस, डिजिटल नेटवर्क, सोशल मीडिया, कंप्यूटर या मोबाइल सॉफ्टवेयर आदि के माध्यम से किए जाते हैं इसमें ऑनलाइन धोखाधड़ी, हैकिंग, साइबर बुलिंग, पहचान की चोरी, साइबर स्टाफिंग, डिजिटल उत्पीड़न, कैट फिशिंग, डाटा ब्रीच, इंसाइडर अटैक, डी डी ओ एस अटैक,वायरस अटैक, मार्फिग डीपफेक, रिवेंजपोर्न, ऑनलाइन सेक्स टॉर्शन, चाइल्ड पोर्नोग्राफी और यौन शोषण, साइबर आतंकवाद जैसी कई अपराधी गतिविधियां शामिल होती है। साइबर अपराध केवल तकनीकी या कानूनी समस्या नहीं है बल्कि इसके पीछे कई गहरे सामाजिक और मनोवैज्ञानिक कारण होते हैं कुछ अपराधी आर्थिक समस्याओं से प्रेरित होते हैं कुछ सामाजिक असमानता का बदला लेना चाहते हैं जबकि कुछ सत्ता

साइबर अपराधियों के द्वारा अपराध किए जाने के सामाजिक पहलू–साइबर अपराध के सामाजिक पहलुओं को दो प्रकार से समझ सकते है–

- **साइबर अपराधियों से संबंधित सामाजिक कारण।**
- **साइबर अपराध से पीड़ित लोगों पर सामाजिक प्रभाव।**

साइबर अपराधियों द्वारा जो साइबर क्राइम किए जाते हैं उनके पीछे निम्न सामाजिक कारण होते हैं –

आर्थिक असमानता और बेरोजगारी –गरीबी और बेरोजगारी से जूझ रहे लोग जल्दी पैसा कमाने के लिए साइबर अपराध का रास्ता अपनाते हैं। ऑनलाइन ठगी, फिशिंग, डिजिटल बैंकिंग फ्रॉड गतिविधियां आर्थिक तंगी के कारण बढ़ती हैं। कुछ लोग सोचते हैं कि अगर वह पारंपरिक नौकरी नहीं पा सकते तो वह इंटरनेट के जरिए अवैध तरीकों से धन कमा सकते हैं इसके लिए वे निम्न तरीके अपनाते हैं–

- **ऑनलाइन ठगी**– नकली वेबसाइट बनाकर लोगों से पैसे ठगना।
- **रैन्समवेयर अटैक**–कंपनियों का डाटा चुराकर फिरौती मांगना।
- **क्रेडिट कार्ड स्कैम**–गरीब और बेरोजगार लोग पैसे के लालच में फर्जी कार्ड ट्रांजैक्शन करते है।

डिजिटल साक्षरता की कमी : समाज के कई वर्गों में डिजिटल जागरूकता की कमी होती है जिससे वे आसानी से साइबर अपराधियों का शिकार बन जाते हैं। कम शिक्षित लोग अक्सर साइबरफ्रॉड,ऑनलाइन ठगी और फेक न्यूज का हिस्सा बन जाते हैं। कई लोग अनजाने में अवैध गतिविधियों में शामिल हो जाते हैं क्योंकि वे इंटरनेट के खतरों को नहीं समझते। डिजिटल साक्षरता की कमी के कारण निम्न प्रकार से साइबर अपराध होते हैं –

- **बैंकिंग फ्रॉड** –फर्जी कॉल और ईमेल के जरिए ठगे जाते हैं क्योंकि इन्हें साइबर सुरक्षा का ज्ञान नहीं होता।
- **फेक न्यूज फैलाना** –बिना जांच पड़ताल किए लोग अफवाहें शेयर करते हैं जिससे समाज में अस्थिरता आती है।
- **डेटा चोरी**–काम डिजिटल ज्ञान रखने वाले लोग अपने बैंक विवरण और पासवर्ड सांझा कर देते हैं जिससे धोखाधड़ी होती हैं।

सामाजिक असमानता और प्रतिशोध–जातीय, धार्मिक या लैंगिक भेदभाव से पीड़ित लोग साइबर अपराध के जरिए समाज से बदला लेने की कोशिश कर सकते हैं। वर्ग संघर्ष के कारण कुछ लोग सरकारी या बड़े कॉरपोरेट संस्थाओं को निशाना बनाते हैं। कुछ साइबर अपराधी निजी दुश्मनी या रिश्तो की समस्याओं के कारण बदला लेने के लिए दूसरों की जानकारी लीक करते हैं। सामाजिक असमानता और प्रतिशोध के कारण निम्न प्रकार से साइबर अपराध होते हैं–

- **हैक्टिविज्म**–किसी राजनीतिक या सामाजिक संगठन के खिलाफ हैकिंग करना।

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

- **साइबर स्टॉकिंग**–प्रेम संबंधों में असफल लोग अपने पूर्व साथी को नुकसान पहुंचाने के लिए ऐसा करते हैं।
- **डेटा लीक और मॉर्फिंग**–किसी की प्रतिष्ठा खराब करने के लिए उसकी तस्वीरों के साथ छेड़छाड़ करना।

इंटरनेट की गुमनामी का फायदा उठाना–इंटरनेट पर बेनामी रहकर अपराध करना आसान हो जाता है क्योंकि अपराधियों को लगता है कि वे पकड़े नहीं जाएंगे। अपराधी बीपीएन टॉर और फर्जी अकाउंट्स का उपयोगकर अपनी पहचान छिपा लेते हैं कुछ लोग सिर्फ मनोरंजन या थ्रिल के लिए साइबर अपराध करते हैं। इसके तहत इन प्रकार से साइबर अपराध होते हैं–

डीपफेक– यह एक एआई तकनीकी है जिसमें किसी व्यक्ति के चेहरे, आवाज या हाव–भाव को नकली तरीके से बदलकर उसे असली जैसा दिखाया जाता है। डीप फेक मशीन लर्निंग और डीप न्यूरल नेटवर्क का उपयोग करके वीडियो, ऑडियो और तस्वीरों को एडिट करता है यह नकली वीडियो और आवाज इतनी वास्तविक लगती है की पहचानना मुश्किल हो जाता है जैसे किसी नेता की फर्जी वीडियो बनाकर गलत बयान दिखाना। किसी की तस्वीर को मॉर्फ करके अश्लील वीडियो में बदलना। किसी की आवाज और चेहरा नकली बनाकर धोखाधड़ी करना।

साइबर बुलिंग और ऑनलाइन उत्पीड़न– साइबर बुलिंग का अर्थ है इंटरनेट, सोशल मीडिया, मोबाइल, ईमेल आदि के जरिए किसी व्यक्ति को मानसिक रूप से परेशान करना, धमकाना या बदनाम करना।

यह निम्न प्रकार से किया जाता है

- **ट्रोलिंग**–सोशल मीडिया पर गालियां देना या गलत टिप्पणियां करना।
- **डॉक्सिंग**–किसी की निजी जानकारी (फोन नंबर, पता) सार्वजनिक करना।
- **मॉर्फिंग**–किसी की तस्वीर के साथ छेड़छाड़ करके बदनाम करना।
- **रिवेंज पॉर्न**–किसी के निजी वीडियो को लीक करना।
- **डार्क वेब**– डार्क वेब एक छिपा हुआ हिस्सा है जो सामान्य सर्च इंजन से एक्सेस नहीं किया जा सकता है और इसके लिए स्पेशल ब्राउजर की जरूरत होती है। डार्क वेब पर वेबसाइटें एनक्रिप्टेड और गुप्त होती हैं जिससे यूजर्स की पहचान छिपी रहती है। इसका इस्तेमाल अवैध गतिविधियां, ड्रग्स, हथियारों की बिक्री, साइबर अपराध और गुप्त संचार के लिए किया जाता है।

ऑनलाइन गेमिंग और सोशल मीडिया का प्रभाव–कई युवा ऑनलाइन गेमिंग और सोशल मीडिया से प्रभावित होकर अपराध की दुनिया में प्रवेश कर जाते हैं गेमिंग और सोशल मीडिया पर साइबर बुलिंग,ठगी और हैकिंग जैसी गतिविधियां बढ़ती हैं कुछ लोग अधिक फॉलोअर्स पाने के लिए फेक न्यूज या विवादित सामग्री पोस्ट करते हैं। इसके तहत इस प्रकार से साइबर अपराध होते हैं–

- **स्वाटिंग**–ऑनलाइन गेमर्स अपने विरोधियों को डराने के लिए पुलिस को झूठी जानकारी देते हैं।
- **चाइल्ड ग्रूमिंग**–अपराधी बच्चों को ऑनलाइन गेम्स और चेटिंग एप्स के जरिए बहला फुसलाकर शिकार बनाते हैं।
- **डिजिटल वेंडेलेज्म**–किसी की सोशल मीडिया प्रोफाइल हैक कर उसे बदनाम करना।

साइबर अपराध के प्रति समाज की उदासीनता–समाज में साइबर अपराध को अभी भी कम गंभीर अपराध माना जाता है जिससे अपराधियों को बढ़ावा मिलता है। कई पीड़ित शिकायत दर्ज नहीं कराते जिससे अपराधी बेखॉफ होकर नए अपराध करते हैं। सरकारी एजेंसियां भी साइबर अपराधियों का हौसला बढ़ाती हैं। बैंक फ्रॉड के मामलों में लोग शिकायत दर्ज कराने में झिझकते हैं। साइबर बुलिंग के पीड़ित अक्सर इसे नजरअंदाज कर देते हैं जिससे अपराधी और सक्रिय हो जाते हैं। फर्जी खबरें फैलाने वाले लोगों को सजा न मिलने के कारण बार–बार ऐसा करते हैं।

साइबर अपराध को आसान और कम खर्चीला समझना–पारंपरिक अपराधों की तुलना में साइबर अपराध करना सस्ता और कम जोखिम भरा होता है। अपराधी को शारीरिक रूप से कहीं जाना नहीं पड़ता बस एक लैपटॉप और इंटरनेट कनेक्शन काफी होता है। कई लोग समझते हैं कि वह दूसरे देशों में बैठकर अपराध करेंगे तो उन्हें पकड़ा नहीं जाएगा। इसके उदाहरण निम्न हो सकते हैं–

- **क्रिप्टोकरेंसी स्कैम**–ब्लॉक चेन टेक्नोलॉजी का गलत इस्तेमाल करके लोगों को ठगना।
- फेक आईडी बनाकर लोगों से ठगी करना।
- बॉटनेट का उपयोग कर बड़े साइबर हमले करना।

तकनीकी कौशल का दुरुपयोग–कई प्रतिभाशाली युवा हैकिंग और कोडिंग में निपुण होते हैं लेकिन वह इन कौशलों का गलत उपयोग करने लगते हैं जैसे–

- **ब्लैक हैट हैकिंग**–वेबसाइट्स और सिस्टम को बिना अनुमति के हैक करना।
- **डाटा लीक** –कंपनियों की गोपनीय जानकारी को सार्वजनिक करना।
- **स्क्रिप्ट किडीज**–बिना गहरे ज्ञान के पहले से मौजूद हैकिंग टूल्स का उपयोग करना।

साइबर अपराध से पीड़ित लोगों पर सामाजिक प्रभावः साइबर अपराध केवल आर्थिक नुकसान ही नहीं पहुंचाता बल्कि पीड़ित के सामाजिक जीवन और संबंधों पर भी गहरा प्रभाव डालता है।

सामाजिक प्रतिष्ठा पर नकारात्मक प्रभाव–अगर कोई व्यक्ति साइबर कूलिंग दीप फेक रिवेंज पूर्ण या फेक न्यूज का शिकार होता है तो उसकी सार्वजनिक छवि खराब हो सकती है समाज में उनका सम्मान कम हो जाता है। लोग उसे शक की नजर से देखने लगते हैं विशेष रूप से महिलाओं और किशोरियों पर इसका प्रभाव अधिक पड़ता है क्योंकि उनकी छवि को लेकर समाज अधिक संवेदनशील होता है।

पारिवारिक और सामाजिक रिश्तों में दरार–साइबर अपराध का शिकार व्यक्ति अपने परिवार और दोस्तों से दूरी बना सकता है परिवार में आपसी तनाव, विश्वास की कमी और कलह बढ़ सकता है। माता–पिता और बच्चों के बीच संचार कम हो सकता है खासकर यदि बच्चा साइबर बुलिंग का शिकार हुआ हो। अगर किसी महिला का डीपफेक वीडियो वायरल हो जाए तो उसका परिवार उसे सपोर्ट करने के बजाय शर्मिंदगी महसूस कर सकता है।

कार्यस्थल पर प्रभाव–साइबर अपराध के कारण किसी कर्मचारी की छवि खराब हो सकती है जिससे उसकी नौकरी पर खतरा आ सकता है किसी व्यक्ति की व्यक्तिगत जानकारी लीक होने पर उसे ब्लैकमेल किया जा सकता है। ऑनलाइन धोखाधड़ी या फेक न्यूज के कारण किसी बिजनेस को नुकसान हो सकता है। किसी कर्मचारी की ई–मेल हैक कर अश्लील सामग्री भेजी जाए तो उसकी नौकरी जा सकती है। किसी कंपनी का डेटा चोरी होने पर ग्राहकों का भरोसा कम हो सकता है।

समाज में विश्वास और डर का माहौल– साइबर अपराधों की बढ़ती घटनाओं से लोगों में डर बढ़ जाता है और वह ऑनलाइन प्लेटफॉर्म पर खुद को असुरक्षित महसूस करने लगते हैं। लोग सोशल मीडिया ऑनलाइन ट्रांजैक्शन और डिजिटल सेवाओं पर भरोसा करने में हिचकिचाने लगते हैं। साइबर स्टॉकिंग के कारण कई महिलाएं सोशल मीडिया से दूरी बना लेती हैं।

न्याय और कानूनी प्रक्रिया में परेशानी–साइबर अपराधों को ट्रैक करना मुश्किल होता है क्योंकि अपराधी का अनाम रह सकते हैं कानूनी प्रक्रिया लंबी और जटिल रह सकती है जिससे पीड़ित को न्याय मिलने में देरी होती है कई बार पीड़ित

सामाजिक बदनामी के दर से शिकायत दर्ज नहीं करवाते हैं बैंकिंग फ्रॉड के मामलों में पैसा वापस पाने की प्रक्रिया लंबी और जटिल होती है।

सामाजिक अलगाव और अकेलापन—साइबर अपराध के शिकार व्यक्ति को समाज से अलग– थलग महसूस होने लगता है। साइबर बुलिंग, ऑनलाइन ट्रोलिंग या डीप फेक वीडियो के शिकार लोग लोग खुद को समाज से दूर करने लगते हैं पीड़ित को लगता है लोग उसे शक की नजर से देख रहे हैं या उस पर हंस रहे हैं। साइबर स्टॉकिंग की शिकार महिलाएं सार्वजनिक जगहों पर जाने से डरती हैं।

सामाजिक शर्मिंदगी—साइबर अपराध के कारण व्यक्ति को समाज में शर्मिंदगी झेलनी पड़ती है किसी महिला की तस्वीर को एडिट करके अश्लील बनाकर सोशल मीडिया पर वायरल कर दिया जाए तो समाज उसे ही दोषी ठहराने लगता है। किसी व्यक्ति का बैंक अकाउंट हैक होकर पैसों की ठगी हो जाए तो उसके परिचित उसे मूर्ख समझने लगते हैं जिससे वे शर्मिंदगी महसूस करते हैं।

साइबर अपराधः एक मनोवैज्ञानिक समस्या—साइबर अपराध के मनोवैज्ञानिक प्रभावों को अपराधियों एवं पीड़ितों दोनों के संदर्भ में समझना जरूरी है क्योंकि अपराधियों के अपराध के पीछे उनकी मनोवैज्ञानिक प्रवृत्तियां होती हैं जो उन्हें अपराध करने के लिए प्रेरित करती है और जो उनके अपराध के पीड़ित होते हैं उन पर भी इन अपराधों का बुरा मनोवैज्ञानिक प्रभाव पड़ता है जिससे उनका मानसिक स्वास्थ्य प्रभावित होता है।

साइबर अपराधियों की अपराध के पीछे की मानसिकता—किसी भी अपराध के पीछे अपराधियों की मानसिकता होती है जो उन्हें अपराध के लिए प्रेरित करती है यह निम्न हो सकती है—

अंतर्मुखी और समाज से कटा हुआ—कई साइबर अपराधी असल जिंदगी में कम बातचीत करने वाले यथार्थ अंतर्मुखी तथा समाज से कटे हुए होते हैं और ऑनलाइन ज्यादा सक्रिय रहते हैं। और साइबर अपराध की ओर उन्मुख होते हैं।

जोखिम लेने की प्रवृत्ति—इनके व्यक्तित्व लक्षणों में जोखिम लेने की प्रवृत्ति पाई जाती है जो बिना किसी डर के कानून तोड़ने का जोखिम लेते हैं उनकी यह प्रवृत्ति उन्हें साइबर अपराध की ओर प्रेरित करती हैं।

मानसिक विकृतियॉ —साइबर अपराधियों में मानसिक विकृतियॉ पाई जा सकती हैं जो उन्हें साइबर अपराध के लिए प्रेरित करती हैं जैसे—

- **नार्सिसिस्टिक प्रवृत्ति**— साइबर अपराधियों में यह प्रवृत्ति पाई जाती है जिसमें खुद को श्रेष्ठ मानना और दूसरों को बेवकूफ बनाने में आनंद महसूस करना। इस प्रवृत्ति से प्रेरित होकर वे साइबर अपराध करते हैं।
- **साइकोपैथी**—निर्दयता और सहानुभूति की कमी— दूसरों की भावनाओं और पीड़ा के प्रति संवेदनहीन होते हैं अपराध बोध नहीं होता है और वह ऑनलाइन धोखाधड़ी, साइबर स्टॉकिंग, साइबर ब्लैकमेलिंग में शामिल होते हैं।
- **सोशियोपेथी**—समाज विरोधी प्रवृत्ति—इस विकृति के कारण वे सामाजिक नियमों और नैतिकता की अनदेखी करते हैं आक्रामक और अस्थिर व्यवहार वाले होते हैं यह साइबरबुलिंग,ट्रोलिंग,ऑनलाइन उत्पीड़न और रिवेंज पोर्न आदि जैसे साइबर अपराध में संलग्न हो सकते हैं।
- **मैकियावेलियनिज्म**—चलाकी और छल कपट—इस विकृति से ग्रसित व्यक्ति में दूसरों को धोखा देने की प्रवृत्ति होती है ये नैतिकता की परवाह नहीं करते और किसी भी हद तक जाकर लक्ष्य प्राप्त करने की मानसिकता से ग्रसित होते हैं। और ये हैकिंग,डेटाचोरी,सोशल इंजीनियरिंग हमले और ऑनलाइन घोटाले में शामिल हो सकते हैं।

● **स्किजोफ्रेनिया–** भ्रम और असामान्य सोच–इस प्रवृति से ग्रसित लोग वास्तविकता और कल्पना के बीच अंतर नहीं कर पाते हैं यह अति भ्रम का अनुभव करते हैं और यह साइबर आतंकवाद सरकारी और सैन्य डेटा हैकिंग और साजिश और गलत सूचना फैलाने में शामिल हो सकते हैं।

● **ऑब्सेसिव कंपल्सिव डिसऑर्डर**–इस विकृति से पीड़ित लोगों में हर चीज को नियंत्रित करने की इच्छा रखते हैं और साइबर स्टॉकिंग, लगातार निगरानी जैसे साइबर अपराध से संबंधित हो सकते हैं।

● **इंटरनेट एडिक्शन डिसऑर्डर**–इस डिसऑर्डर से संबंधित व्यक्ति इंटरनेट का अत्यधिक उपयोग करता है जो पोर्नोग्राफी, हैंगिंग, ऑनलाइन गेमिंग फ्रॉड आदि अपराध में शामिल हो सकता है।

● **एंटी सोशल पर्सनालिटी डिसऑर्डर**–ये डिसऑर्डर वाले व्यक्ति समाज और कानून की परवाह नहीं करते ये साइबर अपराध जैसे साइबर आतंकवाद, डेटा चोरी में संलग्न हो सकते हैं।

● **बाइपोलर डिसऑर्डर**–इस डिसऑर्डर में व्यक्ति के मूड में अत्यधिक बदलाव आता है वह ऑनलाइन उत्पीड़न आदि साइबर अपराध की ओर बढ़ सकते हैं।

डिजिटल नशा और इंटरनेट की लत–डिजिटल नशा और इंटरनेट की लत साइबर अपराध को बढ़ावा देने में महत्वपूर्ण भूमिका निभाती है। सोशल मीडिया की लत से लोग दूसरों की प्रोफाइल बार–बार देखते हैं और उनकी व्यक्तिगत जानकारी इकट्ठाकरते हैं। यह धीरे–धीरे साइबर स्टॉकिंग, उत्पीड़न और ब्लैकमेलिंग में बदल सकता है।

रोमांच और "एड्रेनालाईन रश"–साइबर अपराध के मनोवैज्ञानिक कारणों में "थिल– सीकिंग बिहेवियर" और "एड्रेनालाईन रश" भी है यह वह मानसिक अवस्था है जिसमें व्यक्ति खतरनाक चुनौतीपूर्ण या अवैध गतिविधियों में रोमांस का अनुभव करता है कुछ लोग सिर्फ मनोरंजन या उत्साह के लिए साइबर अपराध करते हैं उन्हें किसी से बदला नहीं लेना होता या आर्थिक लाभ नहीं चाहिए होता बल्कि वे यह देखना चाहते हैं कि वह सिस्टम को कितना तोड़ सकते हैं कई युवा केवल यह देखने के लिए सिस्टम में घुसने की कोशिश करते हैं कि वह कितने कुशल हैं। कुछ लोग बिना अनुमति दूसरों की निजी जानकारी निकालने की कोशिश करते हैं जिससे उन्हें रोमांस महसूस होता है जब कोई व्यक्ति रिस्क या अवैध गतिविधियां करता है तो उसका दिमाग एड्रेनालाईन नामक हार्मोन रिलीज करता है जो उसे उत्तेजना और खुशी महसूस कराता है।

ऑनलाइन डिसइनहिबिशन इफेक्ट–ऑनलाइन डिसइनहिबिशन इफेक्ट एक मनोवैज्ञानिक सिद्धांत है जिसके अनुसार इंटरनेट पर लोग वास्तविक दुनिया की तुलना में अधिक खुलकर आक्रामक या अनैतिक व्यवहार कर सकते हैं इंटरनेट की अनामिता, भौतिक दूरी और त्वरित प्रतिक्रिया की वजह से लोग अपने नैतिक बंधनों को भूलकर ऐसी हरकतें करने लगते हैं जिन्हें वे आमने–सामने कभी नहीं करेंगे। यह प्रभाव दो तरह का हो सकता है–

● **बेनाइन डिसइनहिबिशन**– सकारात्मक प्रभाव–लोग अपनी भावनाएं खुलकर व्यक्त कर सकते हैं। शर्मीले लोग भी आत्मविश्वास से संवाद कर सकते हैं।

● **टॉक्सिक डिसइनहिबिशन**–नकारात्मक प्रभाव–साइबर अपराधी खुद को अज्ञात समझकर अवैध गतिविधियों में लिप्त हो जाता है लोग नैतिकता और कानून के डर के बिना खतरनाक अपराध करते हैं।

साइबर अपराध के पीड़ितों पर पड़ने वाले प्रमुख मनोवैज्ञानिक प्रभाव–साइबर अपराध से पीड़ित होने वाले व्यक्ति निम्न प्रकार से मानसिक रूप से प्रभावित होते हैं–

चिंता और घबराहट –साइबर अपराध का शिकार होने के बाद पीड़ितों में असुरक्षा, भय और अनिश्चितता की भावना विकसित हो सकती है उन्हें यह डर सताने लगता है कि उनकी व्यक्तिगत जानकारी का दुरुपयोग फिर से हो सकता है कई मामलों में पीड़ित को सोशल मीडिया और इंटरनेट से डर लगने लगता है।

अवसाद और आत्म सम्मान की कमी –साइबर बुलिंग, ट्रोलिंग और साइबर स्टॉकिंग के शिकार लोग खुद को कमजोर और असहाय महसूस करने लगते हैं बार–बार अपमान, टिप्पणियां और धमकियां मिलने से उनकी आत्म छवि नकारात्मक हो जाती है कुछ लोग डिप्रेशन में चले जाते हैं और जीवन को बेकार समझने लगते हैं।

पोस्ट– ट्रामैटिक स्ट्रेस डिसऑर्डर–गंभीर साइबर अपराधों जैसे– रिवेंज पोर्न, हैकिंग, ब्लैकमेलिंग और वित्तीय धोखाधड़ी से गुजरे लोगों में पीटीएसडी विकसित हो सकता है पीड़ित व्यक्ति बार–बार उसी घटना को याद करता है और मानसिक रूप से परेशान रहता है अचानक डर, अनिद्रा और बुरे सपने पीटीएसडी के लक्षण हो सकते हैं।

आत्महत्या के विचार और आत्मा हानि –साइबर बुलिंग और ऑनलाइन उत्पीड़न से कुछ पीड़ित इतने मानसिक रूप से टूट जाते हैं ताकि वे आत्महत्या करने के बारे में सोचने लगते हैं कई किशोर और युवा ऑनलाइन बदनामी और सामाजिक अस्वीकार्यता के कारण आत्महत्या कर चुके हैं कुछ पीड़ित लोग खुद को नुकसान पहुंचाने लगते हैं ताकि वह अपने मानसिक दर्द से बच सकें।

क्रोध और बदला लेने की प्रवृत्ति–कुछ पीड़ित लोग साइबर अपराधियों के खिलाफ बदला लेने की सोचने लगते हैं और खुद भी साइबर अपराधों में शामिल हो सकते हैं वे इंटरनेट पर हैकिंग सीखने या गैर कानूनी गतिविधियों में शामिल होने पर प्रयास कर सकते हैं। कुछ लोग अत्यधिक आक्रामक और सामाजिक हो जाते हैं।

अनिद्रा और तनाव–साइबर अपराध के बाद पीड़ित रात में चौन से सो नहीं पाते क्योंकि उनका दिमाग लगातार इस घटना के बारे में सोचता रहता है। कई मामलों में पीड़ित नींद की गोलियां लेने लगते हैं या मानसिक रूप से अस्वस्थ हो जाते हैं।

हाइपर विजिलेंस–साइबर अपराध का शिकार होने के बाद कुछ लोग बहुत अधिक सतर्क हो जाते हैं वह हर ऑनलाइन गतिविधि पर जरूरत से ज्यादा ध्यान देने लगते हैं ईमेल, मैसेज, कॉल आदि यह हाइपर विजिलेंस उन्हें तनाव ग्रस्त और मानसिक रूप से थका सकता है।

व्यक्तिगत और पेशेवर जीवन का प्रभाव–जो लोग साइबर अपराध का शिकार होते हैं वह अपने करियर और शिक्षा पर ध्यान नहीं दे पाते हैं।कार्यस्थल पर उनका आत्मविश्वास कम हो सकता है जिससे उनकी परफॉर्मेंस प्रभावित होती है ।छात्र ऑनलाइन उत्पीड़न के कारण पढ़ाई छोड़ सकते हैं और पेशेवर लोग ऑनलाइन धोखाधड़ी के कारण नौकरी खो सकते हैं।

पहचान संकट और आत्म संदेह–जब कोई व्यक्ति ऑनलाइन बदनाम हो जाता है या उसका डेटा चोरी हो जाता है तो उसे अपनी पहचान को लेकर भ्रम हो सकता है। कुछ मामलों में व्यक्ति को ऐसा महसूस हो सकता है कि वह अब वैसा नहीं है जैसा पहले था इससे उनकी निर्णय लेने की क्षमता प्रभावित हो सकती है और वह हर फैसले पर शक करने लगते हैं।

डिजिटल फोबिया–कुछ पीड़ितों में इंटरनेट और टेक्नोलॉजी का डर विकसित हो सकता है उन्हें इमेल खोलना, सोशल मीडिया का उपयोग करने या ऑनलाइन लेनदेन करने से डर लगता हैं। यह डर करियर, शिक्षा और निजी जीवन पर नकारात्मक प्रभाव डाल सकता है।

अपराध बोध—कई पीड़ित खुद को दोष देने लगते हैं यह भावना विशेष रूप से साइबर स्टॉकिंग, ऑनलाइन ब्लैकमेल और रिवेंज पोर्न के मामलों में अधिक होती है। अपराध बोध के कारण वे दूसरों से परेशानी छुपाने लगते हैं जिससे उनकी मानसिक स्थिति और खराब हो सकती हैं।

साइबर अपराध की रोकथाम के सामाजिक एवं मनोवैज्ञानिक उपाय—साइबर अपराध आज समाज की बढ़ती हुयी समस्या है जिसको रोकने के लिए तकनीकी उपाय के अलावा निम्न सामाजिक एवं मनोवैज्ञानिक उपायों को अपनाकर रोक सकते हैं—

साइबर अपराध की रोकथाम हेतु अपनाये जाने वाले सामाजिक दृष्टिकोण से उपाय—

साइबर सुरक्षा डिजिटल साक्षरता—बहुत से लोग साइबर अपराधों के बारे में पूरी जानकारी नहीं रखते जिससे वह धोखाधड़ी या हैकिंग का शिकार हो जाते हैं। गॉवों, स्कूलों, कॉलेज और दफ्तरों में साइबर सुरक्षा से जुड़े प्रशिक्षण और जागरूकता कार्यक्रम आयोजित किए जाने चाहिए। सरकारी और निजी संगठनों को मिलकर लोगों को मजबूत पासवर्ड, डेटा सुरक्षा, ऑनलाइन फ्रॉड से बचाव आदि के बारे में शिक्षित करना चाहिए।

साइबर अपराधियों के लिए सख्त कानूनी कार्यवाही—साइबर अपराधियों को कठोर दंड देने से अपराध करने की प्रवृत्ति कम होगी। लोगों को यह जानकारी होनी चाहिए कि भारत में आईटी एक्ट 2000 और भारतीय दंड संहिता के तहत कई साइबर अपराधों के लिए कड़ी सजा का प्रावधान है सोशल मीडिया प्लेटफॉर्म्स और टेक कंपनियों को भी जवाबदेह बनाया जाना चाहिए ताकि वे फेक अकाउंट, साइबर बुलिंग और फ्रॉड जैसी समस्याओं पर सख्त कदम उठाएं।

नैतिक शिक्षा और साइबर एथिक्स—बच्चों और युवाओं को यह सिखाना जरूरी है कि वह ऑनलाइन भी वैसा ही आचरण करें जैसा कि असली दुनिया में करते हैं। स्कूलों और महाविद्यालय में डिजिटल नैतिकता को पाठ्यक्रम का हिस्सा बनाया जाना चाहिए।

माता—पिता और परिवार की भूमिका—माता—पिता को अपने बच्चों की ऑनलाइन गतिविधियों पर ध्यान देना चाहिए बच्चों को बताना चाहिए कि वह अनजान लोगों से ऑनलाइन दोस्ती ना करें। और साइबर ठगों से सावधान रहें। पैरेंटल कंट्रोल सॉफ्टवेयर और डिजिटल गाइडलाइंस को लागू किया जाना चाहिए ताकि बच्चों को सुरक्षित इंटरनेट अनुभव मिल सके। बच्चों में आत्म— नियंत्रण और जिम्मेदार डिजिटल नागरिकता विकसित करना चाहिए।

ऑनलाइन धोखाधड़ी और उत्पीड़न के खिलाफ जागरूकता—ऑनलाइन ट्रोलिंग, साइबर स्टॉकिंग और साइबर बुलिंग के मामले बढ़ रहे हैं। पीड़ितों को बोलने और रिपोर्ट करने के लिए प्रोत्साहित किया जाना चाहिए सोशल मीडिया प्लेटफॉर्म्स को सख्त मॉडरेशन नीतियां लागू करनी चाहिए ताकि नफरत फैलाने वाली या अपमानजनक सामग्री को रोका जा सके स्कूलों, महाविद्यालय और कार्य स्थलों में एंटी साइबर बुलिंग पॉलिसी लागू की जानी चाहिए। बैंकिंग फ्रॉड, ई—कॉमर्स, फेक जॉब ऑफर और ऑनलाइन ठगी से बचने के लिए जागरूकता अभियान चलाने चाहिए संभावित साइबर अपराध की घटनाओं को तुरंत साइबर सेल में रिपोर्ट किया जाना चाहिए।

समुदाय सहभागिता और पड़ोस निगरानी—समाज के स्तर पर लोगों को साइबर सुरक्षा के प्रति जागरूक करना चाहिए। सोशल मीडिया और व्हाट्सएप जैसे प्लेटफार्म पर अफवाहों को फैलने से रोकना चाहिए। स्थानीय प्रशासन और समाज को मिलकर साइबर क्राइम हेल्पडेस्क या जागरूकता कार्यक्रम शुरू करने चाहिए।

IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429 Volume 5, Issue 3, April 2025 Impact Factor: 7.67

साइबर अपराध पीड़ितों के लिए सहायता केंद्र–साइबर अपराध का शिकार होने पर बहुत से लोग मानसिक तनाव, शर्मिंदगी और अवसाद का शिकार हो जाते हैं पीड़ितों को मदद देने के लिए काउंसलिंग केंद्र, हेल्पलाइन नंबर और सपोर्ट ग्रुप बनाए जाने चाहिए। सरकार और सामाजिक संगठनों को मिलकर साइबर अपराध पीड़ितों के लिए मानसिक स्वास्थ्य सहायता उपलब्ध करानी चाहिए।

साइबर अपराधियों के पुनर्वास के लिए सुधार कार्यक्रम –कुछ लोग अज्ञानता या मनोरोग प्रवृत्तियों के कारण साइबर अपराध में लिप्त हो जाते हैं उनके लिए सुधार और पुनर्वास कार्यक्रम शुरू किए जाने चाहिए। काउंसलिंग, डिजिटल नैतिकता शिक्षा और साइबर अपराधियों को रोजगार के अवसर देकर उन्हें सही रास्ते पर लाया जा सकता है।

अगर हम उपरोक्त सामाजिक उपायों को प्रभावी तरीके से लागू करें तो हम एक सुरक्षित जागरूक और साइबर क्राइम मुक्त समाज बना सकते हैं।

साइबर अपराध की रोकथाम के मनोवैज्ञानिक उपाय–साइबर अपराध केवल तकनीकि या कानूनी समस्या नहीं है बल्कि इसके पीछे गहरे मनोवैज्ञानिक कारण भी होते हैं अपराधियों की मानसिक प्रवृत्तियां और पीड़ितों की मानसिक स्थिति को समझ कर ही इस समस्या का समाधान किया जा सकता है। इसके लिए प्रभावी मनोवैज्ञानिक उपाय निम्न है–

अपराधियों की मानसिकता को समझना और सुधारना–कई बार साइबर अपराध सिर्फ पैसे कमाने के उद्देश्य से नहीं बल्कि मानसिक विकृति, रोमांच की लत, बदले की भावना या शक्ति प्रदर्शन की प्रवृत्ति के कारण किए जाते हैं ऐसे अपराधियों की मनोवैज्ञानिक प्रोफाइलिंग करके उनकी मानसिक स्थिति को समझा जा सकता है साइबर अपराधियों को सुधारने के लिए काउंसलिंग और नैतिक प्रशिक्षण देना जरूरी है।

इंटरनेट की लत और डिजिटल नषे को रोकना –साइबर अपराध करने वालों में कई लोग इंटरनेट की लत के शिकार होते हैं लोगों को यह सिखाया जाना चाहिए कि वह डिजिटल दुनिया में भी आत्म नियंत्रण बनाए रखें। डिजिटल डिटॉक्स "नो स्क्रीन टाइम" जैसी पहल को बढ़ावा देना चाहिए।

साइबर अपराध रोकने के लिए संज्ञानात्मक व्यवहार थेरेपी –साइबर अपराध करने वाले कुछ लोगों में आवेश नियंत्रण करने की समस्या होती है संज्ञानात्मक व्यवहार थेरेपी के माध्यम से उनके नकारात्मक सोचने के तरीकों को बदला जा सकता है।

साइबर अपराध पीड़ितों के लिए आत्म सम्मान और आत्मविश्वास बढ़ाने के उपाय –साइबर अपराध के शिकार लोग अक्सर अपमानित और असहाय महसूस करते हैं उनके आत्म सम्मान को बढ़ाने के लिए उन्हें साइकोलॉजिकल सपोर्ट ग्रुप्स में शामिल करना चाहिए तथा मानसिक स्वास्थ्य विशेषज्ञों की मदद लेनी चाहिए।

साइबर अपराध पीड़ितों के लिए मानसिक स्वास्थ्य सहायता–साइबर अपराध का शिकार होने पर पीड़ितों को चिंता, अवसाद, आत्म सम्मान की कमी और सामाजिक अलगाव जैसी समस्याओं का सामना करते हैं उन्हें मनोवैज्ञानिक परामर्श, मानसिक स्वास्थ्य सहायता और भावनात्मक समर्थन देना चाहिए।

मनोविकार प्रवृत्ति का उपचार–अक्सर साइबर अपराधियों में विभिन्न मनोविकार प्रवृत्ति जैसे – एएसपीडी, साइकोपैथी, सोशियोपेथी, स्किजोफेनिया, बाईपोलर डिसऑर्डर, नर्सिस्जिम प्रवृत्ति आदि को नियंत्रित करने के लिए सीबीटी और माइंडफुल थेरेपी, डिजिटल हेल्प वर्कशॉप, मनोचिकित्सा, मनोवैज्ञानिक परामर्श, क्रोध प्रबंधन व तनाव प्रबंधन जैसे मनोवैज्ञानिक हस्तक्षेपों का प्रयोग कर उनका उपचार करना चाहिए इसके लिए पहले उनकी पहचान सुनिश्चित की जाए।

विवेचना

साइबर अपराध आधुनिक डिजिटल समाज की एक गंभीर समस्या है जो न केवल तकनीकि बल्कि सामाजिक और मनोवैज्ञानिक स्तर पर भी गहरा प्रभाव डालती है। ऑनलाइन धोखाधड़ी, साइबर बुलिंग,डिजिटल ठगी, डेटा चोरी और ऑनलाइन उत्पीड़न जैसे अपराध तेजी से बढ़ रहे हैं। इन अपराधों के पीछे न केवल आर्थिक या तकनीकी कारक बल्कि मनोवैज्ञानिक प्रवृत्तियां और सामाजिक परिस्थितयाँ भी जिम्मेदार हैं आज डिजिटल युग में कई लोग नैतिक और सही गलत के भेद को नजर अंदाज कर रहे हैं अब साइबर क्राइम आम हो गया है सरकार ने इसके कई कठोर कदम उठाए हैं साइबर क्राइम के लिए प्रत्येक जिले में थाने खोले गए हैं और एक हेल्पलाइन नंबर 1930 जारी किया गया लेकिन केवल सरकारी प्रयासों से साइबर अपराध को नहीं रोका जा सकता इसके लिए समाज में डिजिटल नैतिकता को बढ़ावा देना जरूरी है। समाज में तकनीकी साक्षरता की कमी से कई लोग ऑनलाइन ठगी के शिकार हो रहे हैं इनको साइबर सुरक्षा के प्रति जागरूक किया जाना चाहिए। शिक्षा प्रणाली में डिजिटल नैतिकता और साइबर सुरक्षा को शामिल किया जाना चाहिए। सोशल मीडिया प्लेटफॉर्म्स पर सख्त नियम लागू किए जाने चाहिए। परिवार को बच्चों और किशोर के ऑनलाइन व्यवहार की निगरानी जरूरी है यदि प्रत्येक परिवार में माता–पिता अपने बच्चों के डिजिटल व्यवहार की मॉनिटरिंग करें और उनका मार्गदर्शन करें तो कई प्रकार के साइबर क्राइम कम हो सकते हैं युवाओं को भी अपने जिम्मेदारी समझनी होगी और थ्रिल व रिवेंज की भावना से इसका दुरुपयोग नहीं करना चाहिए। उन्हें अपने में आत्म नियंत्रण और जिम्मेदार डिजिटल नागरिकता विकसित करनी चाहिए। युवाओं को डिजिटल नशा और इंटरनेट की आदत से बचना चाहिए यदि हम युवाओं को इस समस्या से बचा ले तो काफी हद तक हम साइबर क्राइम को कम कर सकते हैं साथ ही समाज में कानूनी जागरूकता तथा सामाजिक जागरूकता को बढ़ावा देकर साइबर अपराध को कम कर सकते हैं अभी हाल ही में साइबर क्राइम के एक नए रूप "डिजिटल अरेस्ट" के काफी मामले संज्ञान में आए जिसको रोकने के लिए भारत सरकार व राज्य सरकारों द्वारा टीवी, रेडियो, अखबारों द्वारा इसके प्रति लोगों को जागरूक किया गया है और वर्तमान में बड़ी संख्या में लोग जागरुक हो रहे हैं। साइबर अपराध रोकने के लिए सामूहिक प्रयास जरूरी है जिसमें जागरूकता नैतिक शिक्षा सामुदायिक सहयोग और कानूनी सख्ती है। अगर समाज और सरकार मिलकर साइबर अपराध की रोकथाम के लिए सही रणनीतियां अपनाये तो एक सुरक्षित और नैतिक डिजिटल समाज का निर्माण किया जा सकता है।

निष्कर्ष

समस्या कितनी भी बड़ी और गहरी क्यों ना हो उसका समाधान आवश्यक होता है उसको कई दृष्टिकोण से समझ कर समाधान खोजा जा सकता है। साइबर अपराध एक जटिल समस्या है जिसका समाधान केवल कानूनी और तकनीकी उपयोग से संभव नहीं है इसके लिए समाज और अपराधियों और पीड़ितों की मानसिकता में बदलाव लाना भी आवश्यक है। सामाजिक स्तर पर नैतिक शिक्षा, डिजिटल साक्षरता और साइबर सुरक्षा कानून को मजबूत करना जरूरी है। वही मनोवैज्ञानिक स्तर पर अपराधियों की मानसिकता को समझकर उन्हें सही दिशा में मार्गदर्शन देना और पीड़ितों को मानसिक सहायता प्रदान करना जरूरी है। इसके साथ ही इंटरनेट की लत को कम करना और साइबर नैतिकता को बढ़ावा देकर डिजिटल संतुलन बनाए रखना आवश्यक है इस प्रकार साइबर अपराध को केवल तकनीकी समस्या न मानते हुए इसके सामाजिक और मनोवैज्ञानिक पहलुओं पर भी ध्यान देने की आवश्यकता है यदि सामाजिक और मनोवैज्ञानिक दृष्टिकोण से भी इस समस्या से निपटा जाए तो काफी हद तक साइबर अपराध की समस्या को कम किया जा सकता हैं।

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, April 2025
Impact Factor: 7.67

REFERENCES

[1]. Anderson, C. A., & Bushman, B. J. (2018). The effects of digital crime on mental health: A review of the literature. Cyberpsychology, Behavior, and Social Networking, 21(3), 123-130.

[2]. Hinduja, S., & Patchin, J. W. (2019). Cyberbullying: Identification, prevention, and response. Journal of Adolescent Health, 64(4), 35-42

[3]. Kshetri, N. (2020). The economics of cybercrime: Causes, consequences, and countermeasures. Journal of Cybersecurity, 6(2), 1-15.

[4]. Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2018). Cyberbullying and its impact on adolescent mental health. Developmental Psychology, 54(5), 781-791.

[5]. Wall, D. S. (2021). Understanding cybercrime: From virtual threats to real-world harms. Crime, Law, and Social Change, 76(3), 275-290.

[6]. Young, K. S. (2019). Internet addiction and its relationship with cybercrime behaviors: A psychological analysis. International Journal of Cyber Psychology, 7(1), 15-32.

[7]. Kartik(2003). Cyber Bulling. International Journal for Multidisciplinary Research. Vol.5(5)Page1-22

[8]. www.ijfmr.com.