साइबर अपराध : एक विश्लेषण

डॉ० कविता वर्मा
असिस्टेंट प्रोफेसर
समाजशास्त्र विभाग
राजकीय महाविद्यालय बी०बी० नगर
बुलन्दशहर (उ०प्र०)
ईमेलः kavitasahdev@gmail.com

सारांश

उपकरण व तकनीक सदैव से ही मानव की सहायता के लिए आविष्कार किए गए हैं। सभ्यता के विकास के साथ–साथ नये उपकरण व तकनीक की खोज व उन्हें प्रयोग में लाने से मानव जीवन सुखमय बनता गया। विज्ञान व प्रौद्योगिकी के द्वारा मानव प्रकृति पर नियन्त्रण पाने में सक्षम हो पाया। इसी कडी में संचार क्रान्ति द्वारा कम्प्यूटर व इन्टरनेट का प्रादूर्भाव भी हुआ, जिसके द्वारा तेजी से मानव जीवन में बदलाव आया। साथ ही मनुष्य अपनी आवश्यकता की पूर्ति में स्वार्थी बन गया, इसी तकनीक व उपकरणों के माध्यम से उससे अपने हित साधने के लिए समाज विरोधी व कानून विरोधी कार्य भी करने लगा। सूचना व तकनीक के इस युग में कम्प्यूटर व इन्टरनेट के माध्यम से जो नवीन अपराध सामने आये उन्हें साइबर अपराध के रूप में जाना जाता है। इस प्रकार के अपराधों का ग्राफ स्थानीय से लेकर वैश्विक पटल पर बढ़ता ही जा रहा है। प्रस्तुत शोध पत्र में 'साइबर अपराध' क्या है? हमारे समाज में यह किस तरह से हो रहा है तथा उनसे बचाव का क्या तरीके हैं, उन्हें प्रस्तुत करने का प्रयास किया गया है।

मूल बिन्दु

अपराध, साइबर अपराध, इन्टरनेट, कम्प्यूटर, प्रौद्योगिकी।

Reference to this paper should be made as follows:

Received: 20.02.2022
Approved: 12.03.2022

डॉ० कविता वर्मा

साइबर अपराध : एक विश्लेषण

RJPP Oct.21-Mar.22,
Vol. XX, No. I,

pp.108-113
Article No. 13

Online available at *:*
https://anubooks.com/rjpp-2022-vol-xx-no-1

अपराध का इतिहास उतना ही प्राचीन है जितना कि सभ्यता का इतिहास। मानव ने जब से सामूहिक जीवन में प्रादूर्भाव किया, तभी से समूह विरोधी कार्य भी करने प्रारम्भ किये। मानव जब अपनी आवश्यकताओं व स्वार्थ की पूर्ति सामूहिक या सामाजिक मान्यता प्राप्त साधनों से नहीं कर पाता तो वह अपनी स्वार्थ सिद्धि के लिए कही न कहीं समाज विरोधी कार्यो को करने की ओर आतूर हो जाता है। सभ्यता के विकास व प्रगति के साथ यह भी देखा गया है कि समाज में जिस स्तर की तकनीक व प्रौद्योगिकी रही है, उसी स्तर के अपराध भी होते हैं, क्योंकि अपराधी भी तो समाज से निकले व्यक्ति है तथा सामूहिक जीवन के भागीदार। मनुष्य जो अपने जीवन में सीखता है उसी प्रवृत्ति के अनुसार जीवन यापन करता है। तकनीकी ज्ञान व प्रौद्योगिकी के युग में अपराध भी तकनीक व प्रौद्योगिकी से प्रेरित हो रहे हैं, अर्थात् अपराध में भी उच्च कोटी के तकनीकी ज्ञान का प्रयोग किया जा रहा है। वर्तमान युग 'सूचना क्रान्ति का युग' है, जिसमें कम्प्यूटर व इन्टरनेट का प्रयोग जीवन के सभी पक्षों में हो रहा है। आज के युग में मनुष्य को सभी कार्य कम्प्यूटर व इन्टरनेट से करने होते हैं, कोरोना काल में इनका महत्व और भी बढ़ गया है। बच्चों के स्कूल की शिक्षा से लेकर सभी सरकारी प्रशासनिक कार्य, पैसो का लेन–देन, सभी सरकारी कल्याणकारी योजनायें, खरीदारी, टिकट की बुकिंग करवाना, अपना सामाजिक समूह बनाना जैसे सोशल मीडिया, स्थानीय देश–विदेश के समाचार, मनोरंजन, आदि आदि अर्थात् जीवन का कोई भी पक्ष ऐसा नही है जिसमें कम्प्यूटर व इन्टरनेट का प्रयोग न हो। तकनीक का रोजमर्रा के जीवन में इतने प्रयोग के कारण अपराध का भी साधन यही तकनीक अर्थात् कम्प्यूटर व इन्टरनेट हो गये हैं। प्रस्तुत शोध पत्र में समाज में हो रहे कम्प्यूटर व इन्टरनेट से होने वाले अपराध अर्थात् साइबर अपराध का विश्लेषण किया गया है, जिसमें यथासम्भव द्वितीयक स्रोतों से उपलब्ध आंकडो का प्रयोग किया गया है।

समाजशास्त्रीय दृष्टिकोण से अपराध मे वह सभी गतिविधियॉ व क्रियाकलाप शामिल है जो समाज की मान्यताओं के विरूद्ध है तथा समाज की व्यवस्था में व्यवधान डालते हैं। इसी परिपेक्ष्य में अपराधशास्त्री मारवर ने कहा है 'सामाजिक दृष्टिकोण से समाज के नियमों का उल्लघंन अपराध माना जाता है, इसे एक असामाजिक कार्य कहा गया है।'[1] इलिएट लथा मैरिल के अनुसार 'अपराध को एक ऐसे समाज विरोधी व्यवहार के रूप में परिभाषिक किया जा सकता है जिसका समूह के द्वारा बहिष्कार किया जाता है तथा जिसके लिए दण्ड़ निर्धारित किया जाता है।'[2]

21वीं सदी के प्रारम्भ से ही संचार क्रान्ति में इन्टरनेट के तेजी से प्रयोग ने मानव जीवन को सुखमय बनाया तथा दिन पर दिन इस पर मानव की निर्भरता बढ़ती ही जा रही है। लेकिन जैसा समाज का स्तर वैसा ही अपराध का।

अतः कम्प्यूटर व इन्टरनेट के माध्यम से समाज विरोधी व कानून विरोधी गतिविधियॉ भी होने लगी जिन्हें साइबर अपराध कहा जाता है। वह अपराध जो कम्प्यूटर इन्टरनेट द्वारा किया जाता है वह साइबर अपराध है।[3] कम्प्यूटर विशेषज्ञ जेवियर गीज के अनुसार 'साइबर अपराध कम्प्यूटर व इन्टरनेट के माध्यम से होने वाला अपराध है, जिसके अंतर्गत जालसाजी, चाईल्ड पोनोग्राफी, साइबर स्टाकिंग शामिल है।'[4]

ब्रिटिश बैंकिंग एसोसिएशन के अनुमान के अनुसार[5] कम्प्यूटर धोखाधडी से प्रतिवर्ष होने वाला विश्वव्यापी नुकसान लगभग 8 से 10 बिलियन डॉलर है। दूसरे प्रकार के क्राइम की तरह इसे भी तीन भागों में बॉटा गया है –

1 मानवीय संवेदनाओं के विरूद्ध अपराध।

2 सम्पत्ति के विरूद्ध अपराध जैसे धोखाधड़ी, जालसाजी, आई0डी0 चोरी करना।

3 सरकारी तन्त्र के विरूद्ध अपराध जैसे अन्तरिक्ष रिसर्च कार्यक्रमों, मिलिट्री या रक्षा संगठनों, परमाणु ऊर्जा संसाधनों के ऑकडे चोरी या हैक करके उन पर राष्ट्र विरोधी बयान जारी करना आदि।

साइबर अपराध को हम सूचना प्रौद्योगिकी के उपकरणों यथा कम्प्यूटर, मोबाइल, लैपटॉप तथा अन्य सम्बन्धित उपकरणों से जो महत्वपूर्ण व्यक्तिगत, प्रशासनिक व सरकारी सूचनाओं के आदान–प्रदान तथा वित्तीय–व्यवसायिक लेनदेन होता है, उनमे असामाजिक व गैर कानूनी प्रयोग के रूप में जान सकते हैं। अतः यह कहा जा सकता है कि साइबर अपराध इलैक्ट्रॉनिक संचार द्वारा जानकारियों के आदान–प्रदान जो कि ई–मेल, ई–व्यापार, ई–प्रशासन तथा सोशल मीडिया के दुरूपयोग से सम्बन्धित है। सरल शब्दों में इसमें असामाजिक व गैर कानूनी कार्यो के लिए इन्टरनेट को एक माध्यम के रूप में प्रयोग किया जाता है। साइबर अपराध को सूचना प्रौद्योगिकी अधिनियम–2000 के अनुसार दण्डित कार्यो के रूप में भी परिभाशित किया जा सकता है। भारतीय दण्ड संहिता की धारा 503, जिसमें ई–मेल द्वारा धमकी देना, धारा 499 अश्लील सन्देश भेजना, धारा 463 इलैक्ट्रोनिक रिकार्ड के साथ छेड़खानी, धारा 420 नकली बेव–साइट द्वारा धोखाधड़ी, धारा 463 नकली ई–मेल भेजना आदि को भी इसी तरह के अपराध के अंतर्गत स्थान दिया गया है।

भारत में साइबर अपराध

भारत में इन्टरनेट का उपयोग जिस गति से बढ़ रहा है उतनी ही तीव्रता से साइबर अपराधों में वृद्धि हो रही है। Malicious Activity by Source: Global Rankng[5] के अनुसार विश्व में भारत साइबर अपराध में चीन व अमेरिका के बाद तीसरे पायदान पर है। राष्ट्रीय अपराध रिकार्ड ब्यूरों के अनुसार[6] भारत में 2020 में साइबर अपराध के 50035 मामले दर्ज किए गए थे जो पिछले वर्ष दर्ज मामलों की तुलना में 11.8 प्रतिशत अधिक है। सोशल मीडिया पर फर्जी सूचना के 578 मामले सामने आए। देश में साइबर अपराध की दर (प्रति एक लाख की आबादी पर घटनाएँ) 2019 में 3.3 प्रतिशत से बढ़कर 2020 में 3.7 प्रतिशत हो गयी। आंकड़ों के अनुसार देश मे 2019 में साइबर अपराध के मामलों की संख्या 44735 थी जबकि 2018 में यह संख्या 27248 थी। वर्तमान में साइबर अपराध में मोबाइल फोन का प्रयोग तेजी से बढ़ता जा रहा है। दिल्ली पुलिस की फ्यूजन एण्ड स्ट्रैटेजिक आपरेशन इकाई के अनुसार 2020 में 70 प्रतिशत साइबर अपराधों में मोबाइल फोन का प्रयोग किया गया जो कि अपराध में प्रयोग किए गये उपकरण में प्रथम स्थान पर रहा, वहीं दूसरे स्थान पर ब्लूटूथ डिबाइस का प्रयोग दूसरे स्थान पर लिए किया गया।[7] डार्क वेब, वाइस ओवर इंटरनेट प्रोटोकॉल सहित जटिल साइबर क्राइम के तरीकों से सुरक्षा एजेसिंयो की चुनौती बढ़ती जा रही है। लगातार बढ़ते साइबर अपराध के मामलों में सबसे ज्यादा मामले धोखाधड़ी के हैं। दूसरे पायदान पर यौन उत्पीड़न से जुड़े मामले हैं।[8]

साइबर अपराध के प्रकार

1 **स्पैम ईमेल–** इस तरह के मेल के द्वारा अपराधी किसी दूसरे के कम्प्यूटर को नुकसान पहुॅचाते है। ऐसे मेल पर क्लिक करते ही कम्प्यूटर सिस्टम में खराबी आ जाती है।

2 **हैंकिंग –** यह बहुत ही प्रचलित रूप है। इसमें दूसरे की निजी जानकारियों की चोरी की जाती है जैसे कि व्यक्ति का पासवर्ड बदलकर फेर बदल करना अर्थात् इसके अंतर्गत अपराधी गैर कानूनी रूप से किसी व्यक्ति की निजी जानकारियों में बिना उसकी जानकारी के प्रवेश कर उसका डाटा चुराता है, खराब करता है या फेरबदल कर देता है। ऐसे अपराधी को हैकर कहा जाता है।

3 **साफ्टवेयर पाइरेसी** – इसमें किसी अच्छे/ब्राइेड साफ्टवेयर की नकल की जाती है, जो कि वैसा होने का दावा करती है, किन्तु उसकी गुणवत्ता व कार्यप्रणाली बहुत ही घटिया होती है। यह मंहगे साफ्टवेयर को सस्ता करके बेचकर लाभ कमाने का तरीका है। इसमें साफ्टवेयर कम्पनियों को आर्थिक नुकसान तो पहॅूचता ही है साथ ही उपभोक्ता को घटिया व निम्न दर्जे का साफ्टवेयर मिलता है, जिसकी कार्यप्रणाली ठीक नहीं होती।

4 **साइबर बुलिंग –** यह इस तरह से है कि आपके घर में आकर बिना किसी बात के आप पर अशोभनीय टिप्पणी की जाये। सामाजिक नेटवर्किंग पर किसी उपभोक्ता पर अशोभनीय टिप्पणी करना, बार–बार धमकियॉ देना, नफरत फैलाने वाली टिप्पणी करना, ताकि वो परेशान हो तथा सभी के सामने शर्मिन्दा होना पड़े। कई बार ऐसी घटनायें किशोर किशोरियों व युवाओं पर नकारात्मक भावनात्मक प्रभाव डालते हैं, जिससे उसका मानसिक स्वास्थ्य भी बाधित होता है।

5 **साइबर स्टाकिंग** – इस तरह के अपराध सोशल मीडिया द्वारा होते हैं और इसका ज्यादातर शिकार किशोर किशोरियॉ होते हैं, जोकि फेसबुक, इस्टाग्राम आदि के माध्यम से इसकी गिरफ्त मे आ जाते हैं। इसमे अभद्र चैटिंग करना, परेशान करने वाले सन्देश बार–बार भेजना और अश्लील सामग्री इत्यादि भेजना।

6 **साइबर फिशिंग –** कम्प्यूटर तथा इन्टरनेट उपभोक्ताओं की महत्वपूर्ण जानकारियों को धोखेबाजी से प्राप्त करने को साइबर फिशिंग कहा गया है। जिस प्रकार दाना देकर मछली को पकड़ा जाता है, उसी प्रकार अपराधी आकर्षक ई–मेल के माध्यम से उपभोक्ता की जानकारी प्राप्त करते है और उसकी जानकारियों का प्रयोग व्यक्तिगत हित में करते है। जैसे बैंक की जानकारियॉ प्राप्त कर पैसे चुराना आदि।

7 **क्रेडिट कार्ड से चोरी करना –** कार्ड की चोरी कर पैसा निकालना, कार्ड की क्लोसिंग करना, कार्ड का नम्बर व पासवर्ड चोरी करके व्यक्ति के कार्ड से पैसे निकाल लिए जाते हैं अथवा अपराधी ऑनलाइन बड़ी खरीदारी कर लेता है। ऐसा कभी–कभी इस तरह से भी होता है कि व्यक्ति एक देश मे हो और उसके कार्ड से चोरी दूसरे देश में हो।

8 **चाइल्ड पोर्नोग्राफी**– अश्लीलता को बढ़ावा देने के लिए बच्चों को भ्रमित करना इसके अंतर्गत आता है। कम्प्यूटर व इन्टरनेट के माध्यम से यौन–कष्त्यों, अश्लील सामग्री का प्रचार–प्रसार पोनोग्राफी में आता है और जब इसका प्रयोग व प्रसार बच्चों पर किया जाता है तो यह चाइल्ड पोनोग्राफी कहलाता है। राष्ट्रीय अपराध रिकार्ड ब्यूरो के अनुसार 2020 में बच्चों के खिलाफ ऑनलाइन अपराधों के कुल 842 मामले आये, जिनमें से 738 मामलें बच्चों के यौन कृत्यों में चिहिंत करने वाली सामग्री को प्रकाशित करने या प्रसारित करने से सम्बन्धित थे।[9]

9 **साइबर वायरस –** अपराधी द्वारा दूसरे व्यक्ति का कम्प्यूटर करप्त करने, उसके जरूरी प्रोग्राम के डाटा को नष्ट करना आदि इसमें शाामिल है। ऐसे में पीड़ित का जरूरी व संचित डाटा व सामग्री तो खराब व नष्ट होती ही है साथ ही उसे आर्थिक हानि भी उठानी पडती है। इसमें वायरस, वर्म, टार्जन, हॉर्स, लॉजिक हॉर्स आदि वायरस शमिल होते हैं।

साइबर अपराध के कारण

1 जिस गति से इन्टरनेट उपभोक्ता बढ़ते जा रहे हैं उस गति से उनमें सावधानी व डिजिटल जागरूकता नहीं बढ़ रही।

2 अभी भी साइबर अपराध से सम्बन्धित प्रभावी कानूनों की कमी है।

3 साइबर अपराध सेल में तकनीकी/दक्ष अधिकारियों व कर्मचारियों की कमी है।

4 साइबर अपराध से सम्बन्धित शिकायत प्रणाली भी अभी पूरी तरह दुरस्त नही है।

5 कई बार आपसी द्वेश की भावना भी इन अपराधों को बढ़ावा देती है।

6 आर्थिक अपराधों की तरह अधिक धन का लालच भी इस प्रकार के अपराध का कारण है।

7 कम्प्यूटर, मोबाइल व इन्टरनेट उपभोक्ताओं की लापरवाही व असावधानी भी ऐसे अपराधों को न्यौता देती है।

भारत में साइबर अपराध रोकने के तरीके

हमारे देश मे बढ़ते साइबर अपराध, कानून व सुरक्षा एजेंसियों के लिए गम्भीर समस्या बनी हुई है। इनसे बचने के लिए साइबर सुरक्षा के तरीकों को अपनाया जा रहा है। साइबर सुरक्षा का तात्पर्य साइबर स्पेस की हमले, क्षति, दुरूपयोग आदि से सुरक्षा प्रदान करना हैं साइबर अपराध चूँकि अन्तर्राष्ट्रीय स्तर पर बढ़ता जा रहा है। अतः आवश्यकता इस बात की है कि सभी देश एक साथ मिलकर इसके लिए प्रयास करें। इसी दिशा में 2004 मे बुडापेस्ट से अवांछित साइबर गतिविधियों को रोकने के लिए एक सम्मलेन का आयोजन किया गया, जिसका उद्देश्य साइबर अपराध से सुरक्षा प्रदान करवाने के लिए सामान्य नीति बनाना था। हमारे देश में साइबर अपराधों की बढ़ती संख्या को देखते हुए समय–समय पर इस दिशा में प्रयास हुए हैं। सूचना प्रौद्योगिकी (संशोधन) अधिनियम 2008, भारत की नयी साइबर नीति–2003 सूचना प्रौद्योगिकी विभाग द्वारा साइबर सुरक्षा के लिए एक संस्थान 'सर्ट इन' आदि का प्रावधान किया गया है। इन अपराधां से सुरक्षा व निवारण के लिए भारत में सूचना तकनीकी कानून 2008 के निम्न प्रावधान दिये गये हैं[10]–

1 कम्प्यूटर के संसाधनों से छेड़छाड़ की कोशिश (धारा65)

2 कम्प्यूटर में संग्रहित डाटा के साथ छेड़छाड कर उसे हैक करने की कोशिश (धारा66)

3 संवाद सेवाओं के माध्यम से प्रतिबाधित सूचनाएँ भेजने के लिए दण्ड का प्रावधान (धारा66ए)

4 कम्प्यूटर या अन्य किसी इलैक्ट्रोनिक गैजेट से चोरी की गयी सूचनाओं को गलत तरीके से हासिल करने के लिए दण्ड का प्रावधान (धारा66बी)

5 किसी की पहचान चोरी करने के लिए दण्ड का प्रावधान (धारा66सी)

6 अपनी पहचान छुपाकर कम्प्यूटर की मद्द से किसी के व्यक्तिगत डाटा तक पहुँच बनाने के लिये दण्ड का प्रावधान (धारा66डी)

7 किसी की निजवा भंग करने के लिए दण्ड का प्रावधान (धारा66ई)

8 साइबर आतंकवाद के लिए दण्ड का प्रावधान (धारा66एफ)

9 आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े प्रावधान (धारा67)

10 इलैक्ट्रोनिक माध्यमों से अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दण्ड का प्रावधान (धारा67ए)

11 इलैक्ट्रोनिक माध्यमों से आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो। (धारा67बी)

12 मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दण्ड का प्रावधान (धारा67सी)

13 डाटा को गलत तरीके से पेश करना (धारा71)

14 कॉन्ट्रैक्ट की शर्तो का उल्लघंन कर सूचनाओं को सार्वजनिक करने संबंधी प्रावधान (धारा72ए)

15 फर्जी डिजिटल हस्ताक्षर का प्रकाशन (धारा73ए)

इस कानून की धारा 78 मे इस्पेक्टर स्तर के पुलिस अधिकारी को इन मामलों मे जॉच करने का अधिकार प्राप्त है।

निष्कर्ष

वर्तमान में उच्च सूचना तकनीक के युग में सभी व्यक्ति मोबाइल व कम्प्यूटर के माध्यम से इन्टरनेट से जुड़े हुए हैं तथा ये सभी उपकरण व तकनीक हमारे जीवन का अहम् भाग बन गयी है और नित्यप्रति दिन के कार्य इनके बिना होना सम्भव ही नही है। ऐसी स्थिति में इन उपकरणों से सम्बन्धित अपराधों से बचने का एकमात्र उपाय सावधानी व उचित डिजिटल जानकारी ही है। समय–समय पर पुलिस व प्रशासन द्वारा भी इन

अपराधों से बचने के संदेश आते रहते हैं, उनका उचित ढ़ंग से पठान करना चाहिए। यूनिक पासवर्ड और एन्टी वायरस सॉफ्टवेयर का उपयोग करना चाहिए तथा संदिग्ध ई–मेल और अज्ञात लोगों से आने वाले प्रोग्रामों को नहीं खोलना चाहिए। सोशल मीडिया पर अपनी व्यक्तिगत जानकारी नहीं साझा करनी चाहिए। साइबर अपराध से बचने के लिए कम्प्यूटर व स्मार्ट फोन निर्माता कम्पनियॉ भी उपकरण की सुरक्षा बढ़ाने के लिए बायोमीट्रिक्स तकनीक का प्रयोग करने लगी है। इसके लिए फिंगरप्रिंट स्कैकनर, रिकॉर्डिनिशन, आयरिस स्कैन आदि सुविधाओं के प्रयोग के द्वारा इन अपराधों से बचा जा सकता है। अपने उपकरणों, पैसे के लेन–देन से सम्बन्धित एप, प्रोग्राम व स्मार्ट कार्ड के पासवर्ड आदि बदलते रहना चाहिए तथा उन्हें किसी के साथ साझा नहीं करना चाहिए। इस प्रकार के अपराधों से बचने के लिए व्यक्ति को स्वयं तकनीकी रूप से नवीनीकृत करते रहना चाहिए।

संदर्भ

1. Arnest, Mowrer. (1969). "Disorganisation: Social and Personal". Newyork: **Pg. 42-48.**
2. Elliott. and Merrill. (1934). "Social Disorganization". Newyork: **Pg. 542-543.**
3. राजीव, रंजन. (2016). 'कम्प्यूटर ज्ञान एवं सूचना प्रौद्योगिकी'. उपकार प्रकाशानः आगरा. **पृष्ठ 172.**
4. ललिता, शाक्य. (2015). 'साइबर अपराध एक आकलन'. Journal of Asia for Democracy and Development. Vol. –XV, No. 04. **पृष्ठ 78.**
5. (2016). www.cyber crime report.
6. www.togindia.com>India.
7. (2022). हिन्दुस्तान, 17 फरवरी. **पृष्ठ 08.**
8. (2022). हिन्दुस्तान, 17 फरवरी. **पृष्ठ 15.**
9. www.dnaindia.com>DNAIndia>भारत.
10. http://hi.mi:wikipedia.org.