भारतीय समाज में साइबर अपराध की अवधारणा

डॉ. हरिचरण मीना

व्याख्याता समाजशास्त्र विभाग
राजकीय स्नातकोत्तर महाविद्यालय सवाईमाधोपुर

शोध सारांश

साइबर अपराध एक ऐसा अपराध है जिसमें कम्प्यूटर और नेटवर्क शामिल होता है। साइबर अपराध में कम्प्यूटर प्रौद्योगिकी के ज्ञान का दुरुपयोग कानून विरोधी और अनैतिक कार्यो के लिए किया जाता है। इसमें कम्प्यूटर तकनीक से सम्बन्धित प्रतिभावान व्यक्ति कम्प्यूटर का दुरुपयोग करके विभिन्न ऑकड़ों और सामग्रियों को अवैध, अनैतिक और अनधिकृत रुप से संसाधित और सम्प्रेषित करने का काम करते हैं। आधुनिक युग में स्पैम ईमेल, हैकिंग, फिशिंग, वायरस फैलाना, सॉफ्टवेयर पाइरेसी, फर्जी बैंक कॉल, सोशल नेटवर्किंग साइटों पर अफवाह फैलाना, साइबर बुलिंग जैसी साइबर अपराध पूरे विश्व के लोगों के सामने एक गम्भीर समस्या पैदा की है जिसने मानवीय जीवन को भयावह एवं अक्रान्त बना दिया है।

मुख्य शब्द –

साइबर अपराध, स्पैम ईमेल, हैकिंग, फिशिंग, वायरस फैलाना, साफ्टवेयर पाइरेसी, फर्जी बैंक कॉल, सोशल नेटवर्किंग साइटों पर अफवाह फैलाना, साइबर बुलिंग; भारतीय दण्ड संहिता में साइबर अपराधों से संबंधित प्रावधान, सूचना तकनीक कानून 2000 के अन्तर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान।

उद्देश्य – साइबर अपराध के बारे में विस्तार से जानकारी प्राप्त करना।

प्रस्तावना

वर्तमान युग में वैज्ञानिक तथा प्रौद्योगिकी विकास ने जहाँ एक ओर पूरे विश्व को एक वैश्विक गाँव के रुप में बदल दिया है वहीं दूसरी ओर साइबर अपराध के रुप में सम्पूर्ण विश्व के सामने अनेक नई चुनौतिया उत्पन्न की है। आधुनिक युग में कम्प्यूटर से सम्बन्धित टेक्नोलॉजी के कारण हम कुछ ही क्षणों में दुनिया भर में कहीं भी सन्देशों का आदान प्रदान कर सकते

सभी तरह की सूचनाएं प्राप्त कर सकते हैं। कुछ समय पहले तक जिन ऑकड़ों, सूचनाओं और तथ्यों को सुरक्षित रखने के लिए कार्यालयों में हजारों फाइलें रखी जाती थीं, वहीं आज कम्प्यूटर की सहायता से हम सभी ऑकड़े एक साफ्टवेयर में रखकर उसका कभी भी उपयोग कर सकते हैं। आज नेटवर्किंग के माध्यम से एक–दूसरे से हजारों किलोमीटर दूर स्थापित कम्प्यूटरों को एक–दूसरे से इस तरह जोड़कर रखा जा सकता है कि एक साइट से सम्बन्धित सामग्री का उपयोग दूसरे सभी कम्प्यूटरों द्वारा किया जा सकता है।

यह आधुनिकता की दिशा में होने वाली एक ऐसी उपलब्धि है जिसने प्रौद्योगिकी, औद्योगीकरण, वैज्ञानिक विकास, आन्तरिक तथा बाह्य सुरक्षा एवं जीवन के सभी पक्षों को प्रभावित किया है। कम्प्यूटर से जुड़ी आधुनिक टेक्नोलाजी से जहाँ एक ओर व्यापक लाभ हुए है वहीं दूसरी ओर इससे अपराधों में भी वृद्धि हुई है। यह वे साइबर अपराध हैं जो मानवाधिकारों का हनन करने के अतिरिक्त मानवीय मूल्यों के लिए एक बड़ा खतरा बन गए हैं।

साइबर अपराध एक ऐसा अपराध है जिसमें कम्प्यूटर और नेटवर्क शामिल होता है। किसी भी कम्प्यूटर का अपराधिक स्थान पर मिलना या कम्प्यूटर से कोई अपराध करना कम्प्यूटर अपराध कहलाता है।

कम्प्यूटर अपराध में नेटवर्क शामिल नहीं होता है। किसी की निजी जानकारी को प्राप्त करना और उसका गलत इस्तेमाल करना। किसी की भी निजी जानकारी को कम्प्यूटर से निकाल लेना या चोरी कर लेना भी साइबर अपराध कहलाता है। कम्प्यूटर अपराध भी कई प्रकार से किये जाते है जैसे कि जानकारी चोरी करना, जानकारी मिटाना, जानकारी में फेरबदल करना, किसी की जानकारी को किसी और को देना या कम्प्यूटर के भागो को चोरी करना या नष्ट करना।

साइबर अपराध भी कई प्रकार के है जैसे कि स्पैम ईमेल, हैंकिग, फिशिंग, वायरस को डालना, किसी की जानकारी को ऑनलाइन प्राप्त करना या किसी पर हर वक्त नजर रखना।

जब कम्प्यूटर प्रौद्योगिकी के ज्ञान का दुरुपयोग कानून विरोधी और अनैतिक कार्यो के लिए किया जाता है तब ऐसे व्यवहार को हम साइबर अपराध कहते है। जब कम्प्यूटर तकनीक से सम्बन्धित प्रतिभावान व्यक्ति कम्प्यूटर का दुरुपयोग करके विभिन्न ऑकड़ों और सामग्रियों को अवैध, अनैतिक और अनाधिकृत रुप से संसाधित और सम्प्रेषित करने का काम करते हैं, तब ऐसे कार्य को कम्प्यूटर अपराध या साइबर अपराध कहा जाता है।

साइबर अपराध की विशेषताएँ–

(1) साइबर अपराध एक तरह की कम्प्यूटर जालसाजी है।
(2) इसकी प्रकृति अत्यधिक गुप्त और एकाकी होती है।
(3) साइबर अपराध को पकड़ पाना बहुत कठिन होता है।
(4) साइबर अपराध के लिए कम्प्यूटर प्रौद्योगिकी का उच्च ज्ञान आवश्यक है।
(5) ऐसे अपराध प्रौद्योगिक रुप से प्रशिक्षित व्यक्तियों द्वारा ही किये जाते है।

साइबर अपराध के उद्देश्य –

वर्तमान जीवन में साइबर अपराधों के क्षेत्र में लगातार वृद्धि होती जा रही है। इन अपराधों के उद्देश्यों का सम्बन्ध आर्थिक, सैनिक, सांस्कृतिक अथवा व्यक्तिगत किसी भी पक्ष से हो सकता है। इसके प्रमुख उद्देश्य हैं–

(1) किसी विशेष देश के द्वारा दूसरे देश की सैनिक जासूसी करना तथा रक्षा सम्वन्धी सूचनाओं की चोरी करके एक विशेष देश को लाभ पहुचाना होता है।

(2) बड़े–बड़े उद्योगपति भी दूसरे उद्योगपतियों के फार्मूले, पेटेन्ट और बाजार सम्बन्धी सूचनाएँ चोरी करने के लिए कम्प्यूटर प्रौद्योगिकी के उच्च ज्ञान से सम्बन्धित लोगों की सेवाओं का उपयोग करते हैं।

(3) वैश्वीकरण व उदारीकरण के दौर में विभिन्न देशों के बीच होने वाली आर्थिक प्रतिस्पर्धा में साइबर अपराध एक प्रभावशाली साधन बनता जा रहा है।

(4) साइबर अपराध का एक प्रमुख उद्देश्य किन्ही दो देशों के बीच के राजनीतिक और आर्थिक सम्बन्धों में टकराव पैदा करना है। इसके लिए किसी विशेष देश की कूटनीति से सम्बन्धित तथ्यों की चोरी करके उनका दूसरे देश में इस तरह सम्प्रेषण कर दिया जाता है जिससे दोनों के बीच सन्देह और मतभेद की दशा उत्पन्न हो जाए।

(5) साइबर अपराध का एक प्रमुख उद्देश्य प्रमुख राजनीतिक दलों की गुप्त सूचनाए, प्रमुख राजनीतिज्ञों की वार्ता और गतिविधियों की जानकारी दूसरे राजनीतिक दल को देकर उसके हितों को हानि पहुँचाना है।

(6) इसका एक विशेष आर्थिक उद्देश्य बड़े–बड़े इलैक्ट्रॉनिक जुआघरों की व्यवस्था तथा संचालन करना है।

साइबर अपराध के प्रकार –

(01) स्पैम ईमेल – अनेक प्रकार के ईमेल आते है जिससे ईमेल भी होते है जो सिर्फ कम्प्यूटर को नुकसान पर है। उन ईमेल से सारे कम्प्यूटर में खराबी आ जाती है।

(02) हैकिंग – किसी की भी निजी जानकारी को हैक कर जैसे की उपयोगकर्ता का नाम या पासवर्ड और फिर उसमें फेर बदल करना।

(03) फिशिंग – किसी के पास स्पैम ईमेल भेजना ताकि वो अपनी निजी जानकारी दे और उस जानकारी से उसको नुकसान हो सकें। यह ईमेल आकर्षित होते है।

(04) वायरस फेलाना – साइबर अपराधी कुछ ऐसे सॉफ्टवेयर आपके कम्प्यूटर पर भेजते हैं जिसमें वायरस छिपे हो सकते हैं, इनमें वायरस वर्म, टार्जन हार्स, लाजिक हार्स आदि वायरस शामिल हैं। यह आपके कम्प्यूटर को काफी हानि पहुँचा सकता हैं।

(05) सॉफ्टवेयर पाइरेसी – सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है। इससे साफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ता है साथ ही साथ आपके कीमती उपकरण भी ठीक से काम नहीं करते हैं।

(06) फर्जी बैंक कॉल – आपको जाली ईमेल, मैसेज या फोन कॉल प्राप्त हो जो आपकी बैंक जैसा लगे जिसमें आपस पूछा जाये कि आपके एटीम नंबर और पासवर्ड का आवश्यकता है और यदि आपके द्वारा यह जानकारा न दी गयी तो आपका खाता बन्द कर दिया जाएगा या लिंक पर सूचना दें।

हालांकि किसी भी बैंक द्वारा ऐसी जानकारी कभी भी नह मांगी जाती है और भूलकर भी अपनी किसी भी इस प्रकार की जानकारी को इन्टरनेट या फोन काल ये माध्यम से नहीं बताये।

(07) सोशल नेटवर्किंग साइटों पर अफवाह फैलाना– बहुत से लोग सोशल नेटवर्किंग साइटों पर पारिवारिक, सामाजिक, सांस्कृतिक, धार्मिक, राजनीतिक अफवाह फैलाने का काम करते हैं, लेकिन यूजर्स उनके इरादें समझ नहीं पाते हैं और जाने–अनजाने में ऐंसे लिक को शेयर करते रहते हैं, लेकिन यह भी साइबर अपराध और साइबर आतंकवाद की श्रेणी में आते हैं।

(08) **साइबर बुलिंग** –

फेसबुक जैसी सोशल नेटवर्किंग साइटों पर अशोभनीय कमेंट करना, इंटरनेट पर धमकियां देना किसी का इस स्तर तक मजाक बनाना कि तंग हो जाये, इंटरनेट पर दूसरों के सामने शर्मिंदा करना, इसे साइबर बुलिंग कहते हैं । अक्सर बच्चे इसका शिकार होते है। इससे इनके सेहत पर भी असर पड़ता है।

भारतीय दण्ड संहिता (IPC) में साइबर अपराधों से है संबंधित प्रावधान – (1) ईमेल के माध्यम से धमकी भरे संदेश भेजना–IPC article 503 (2) ईमेल के माध्यम से ऐसे संदेश भेजना जिससे मानहानि होती हो–IPC article 499 (3) फर्जी इलेक्ट्रानिक रिकार्डस का इस्तेमाल–IPC article 463 (4) फर्जी – वेबसाइट या साइबर फ्रॉड का इस्तेमाल–IPC article 420 (5) चोरी–छुपे किसी के ईमेल पर नजर रखना–IPC article 463 (6) वेब जैकिंग–IPC article 463 (7) ईमेल का गलत के इस्तेमाल–IPC article 383 (8) दवाओं को ऑनलाइन का बेचना–NDPS act (9) हथियारों की ऑनलाइन खरीद–बिक्री arms act.

सूचना तकनीक कानून, 2000 के अन्तर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान –

इक्कीसवीं शताब्दी में मानव र समाज के विकास की दृष्टि से सूचना एवं संचार तकनीकों की खोज को सबसे महत्वपूर्ण आविश्कार माना जा सकता है। सामाजिक विकास के विभिन्न क्षेत्रों, खासकर न्यायिक प्रक्रिया में – इसके इस्तेमाल की महत्ता को कम करके आंका नहीं जा सकता,। क्योंकि इसकी तेज गति, कई छोटी मोटी दिक्कतों से छुटकारा, – मानवीय गलतीयों की कमी, कम खर्चीला होना जैसे गुणों के चलते यह न्यायिक प्रक्रिया को विश्वसनीय बनाने में अहम भूमिका निभा सकती है।

इतना ही नहीं ऐसे मामलों के निष्पादन में जहाँ सभी संबद्ध पक्षों की शारीरिक उपस्थिति अनिवार्य न हो, यह सर्वश्रेष्ठ विकल्प हो सकता है। सूचना तकनीक कानून के अन्तर्गत उल्लिखित आरोपों की सूची निम्न है–(1) कम्प्यूटर संसाधनों से छेड़छाड़ की कोशिश – धारा 65 (2) कम्प्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश– धारा 66 (3) संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान धारा 66 ए (4) कम्प्यूटर या अन्य किसी इलेक्ट्रानिक गैजेट से चोरा की गई सूचनाओं का गलत तरीके से हासिल करने के लिए दंड प्रावधान–धारा 66 बी (5) किसी की निजता को भंग करने के लिए दंड का प्रावधान–धारा इ (6) आपत्तिजनक सुचनाओं क प्रकाशन से

जुड़े प्रावधान–धारा 67 (7) इलेक्ट्रानिक या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने का प्रावधान दृधारा 67 ए (8) फर्जी डिजिटल हस्ताक्षर का प्रकाशन प्रावधान –धारा 73।

साइबर अपराध रोकने के उपाय –

साइबर अपराध पर नियन्त्रण रखने के लिए कुछ विशेष उपाय करना अत्यन्त आवश्यक है जो निम्न हैं–

(1) साइबर अपराध को रोकने के लिए कम्प्यूटर प्रौद्योगिकी का उच्च ज्ञान रखने वाली एक प्रशिक्षित टीम को संगठित करना आवश्यक है। किसी भी प्रकार के साइबर अपराध की सूचना मिलने पर इसके द्वारा अपराध के स्रोत की जानकारी प्राप्त करके अपराधी को दण्डित किया जा सकता है।

(2) सरकार द्वारा ''सूचना प्रौद्योगिकी अधिनियम'' पारित करने से यह आशा की गई थी कि इसकी सहायता से साइबर अपराध को कम करने में इसकी उपयोगी भूमिका हो सकेगी। इसके बाद भी यह अधिनियम इस कारण प्रभावपूर्ण नहीं बन सका कि इससे सम्बन्धित अधिकांश प्रावधान अधिक व्यावहारिक नहीं है। वर्तमान में इस अधिनियम को अधिक व्यावहारिक बनाने की जरुरत है ताकि साइबर अपराधियों को अति शीघ्र दण्डित किया जा सके।

(3) कम्प्यूटर द्वारा गबन व जालसाजी जैसे अपराधो को तभी कम किया जा सकता है जब विभिन्न लेखा परीक्षकों के लिए कम्प्यूटर का उच्च स्तरीय ज्ञान आवश्यक हो। बड़ी–बड़ी कम्पनियों और बैंको के सभी आकड़े अब कम्प्यूटर में ही सुरक्षित रहते हैं। इस दशा में कम्प्यूटर के ज्ञान के बिना उनके खाते की समुचित ढ़ग से परीक्षा नहीं की जा सकती है।

(4) संसार के विभिन्न देशों में साइबर अपराध को मानवाधिकार उल्लंघन से जुड़ा हुआ अपराध मानकर इसके लिए कठोर दण्ड की व्यवस्था की गई है। भारत में भी इस माडल को अपनाकर साइबर अपराध में कमी की जा सकती है।

(5) अधिकांश कम्प्यूटर अपराध किसी न किसी प्रकार के पासवर्ड की चारी के द्वारा किये जाते हैं। महत्वपूर्ण अपराधों की चोरी रोकने के लिए यह आवश्यक है की पासवर्ड जटिल प्रकार के हों तथा इनकी जानकारी केवल इनका उपयोग करने वाले व्यक्ति अथवा संस्था को ही हो।

निष्कर्ष –

आधुनिक युग में सूचना एवं संचार प्रौद्योगिकी ने जहाँ समाज के हर पहलू को सकारात्मक रुप से प्रभावित किया है वहीं साइबर अपराध ने समाज के सामने एक वैश्विक समस्या प्रस्तुत की है जिसका समाधान अति आवश्यक है।

हांलाकि साइबर अपराध की प्रकृति इतनी एकाकी और अज्ञात होती है कि इनसे सम्बन्धित वास्तविक अपराधी को खोज पाना एक कठिन समस्या है। साइबर अपराध के विरुद्ध यदि प्रारम्भिक स्तर पर ही पर्याप्त कार्यवाही नहीं की जाती है तो मानवाधिकारों और मानवीय मूल्यों का हनन होने से समाज में विघटनकारी मनोवृत्तियों का तेजी से विकास होने लगेगा। यह एक ऐसी दशा है जिसमें भावी समाज का सम्पूर्ण जीवन एक बड़े खतरे में पड़ सकता है।

सन्दर्भ सूची

1. Jain, Rohit Arvind (2018) “Cyber Crime & Law", Evincepub Publishing. ISBN&109789387905726
2. Chander, Harish, “Cyber Laws and IT Protection
3. Dr. Agrawal, G.K., “Sociology” SBPD Publishing House
4. Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations-.Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
5. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.