शोध मंथन Vol. XI No.I Jan.-Mar. 2020 ISSN: (P) 0976-5255 (e) 2454-339X
Impact Factor 7.760 (SJIF)

साइबर एक अपराध

डॉ0 अनिता रानी,
एसो0 प्रोफे0, संगीत विभाग, सितार,
बी0डी0 जैन गर्ल्स पी0जी0 कालिज, आगरा
Email: dr.anita80@gmail.com

सारांश

साइबर अपराध एक ऐसा अपराध है जिसमें कंप्यूटर और नेटवर्क दोनों शामिल हैं। किसी भी कंप्यूटर का आपराधिक स्थान पर मिलना या कंप्यूटर से कोई अपराध करना कंप्यूटर अपराध कहलाता है। कंप्यूटर अपराध में नेटवर्क शामिल नहीं होता है। किसी की निजी जानकारी प्राप्त करना और उसका गलत इस्तेमाल करना, किसी की भी निजी जानकारी कंप्यूटर से निकाल लेना या चोरी कर लेना यह सब भी साइबर अपराध ही है।

प्रस्तावना

साइबर अपराध एक ऐसा अपराध है जिसमें कंप्यूटर और नेटवर्क दोनों शामिल हैं। किसी भी कंप्यूटर का आपराधिक स्थान पर मिलना या कंप्यूटर से कोई अपराध करना कंप्यूटर अपराध कहलाता है। कंप्यूटर अपराध में नेटवर्क शामिल नहीं होता है। किसी की निजी जानकारी प्राप्त करना और उसका गलत इस्तेमाल करना, किसी की भी निजी जानकारी कंप्यूटर से निकाल लेना या चोरी कर लेना यह सब भी साइबर अपराध ही है।

कंप्यूटर अपराध भी कई प्रकार से किये जाते हैं जैसे कि जानकारी चोरी करना, जानकारी मिटाना, जानकारी में फेर बदल करना, किसी की जानकारी को किसी और का बना देना या कंप्यूटर के भागों को चोरी करना या नष्ट करना। साइबर अपराध भी कई प्रकार के हैं जैसे कि स्पैम ईमेल, हैकिंग, फिशिंग, वायरस को डालना, किसी की जानकारी को ऑनलाइन प्राप्त करना या हर वक्त नजर रखना।

कंप्यूटर अपराध के प्रकार–

जानकारी चोरी करना– किसी के कंप्यूटर से उसकी निजी जानकारी निकालना जैसे कि उपयोगकर्ता का नाम या पासवर्ड

जानकारी मिटाना– किसी के कंप्यूटर से जानकारी मिटाना ताकी उसे नुकसान हो या कोई जरूरी जानकारी को मिटाना।

फेर बदल करना– जानकारी में कुछ हटाना या जोड़ना, उस जानकारी को बदल देना।

बाहरी नुकसान– कंप्यूटर के भागों को नष्ट करना, उसे तोड़ना या भागों की चोरी

करना भी कंप्यूटर अपराध में आता है।

साइबर अपराध के प्रकार

• **स्पैम ई–मेल –** अनेक प्रकार के ईमेल आते हैं जिसमें ऐसे ईमेल भी होते हैं जो सिर्फ कंप्यूटर को नुकसान पहुचाते हैं। उन ईमेल से सारे कंप्यूटर में खराबी आ जाती है।

• **हैकिंग–** किसी की भी निजी जानकारी को हैक करना जैसे कि उपयोगकर्ता का नाम या पासवर्ड में फर बदल करना।

• **फिशिंग**– किसी के पास स्पैम ईमेल भेजना ताकी वो अपनी निजी जानाकरी दे सके और उस जानकारी से उसका नुकसान हो सके।

• **वायरस फैलाना –** साइबर अपराधी कुछ ऐसे सॉफटवेयर आपके कंप्यूटर पर भेजते हैं जिसमें वायरस छिपे हो सकते हैं, इनमें वायरस, वर्म, टार्जन हॉर्स, लाजिक हार्स आदि वायरस शामिल है, यह आपके कंप्यूटर को काफी हानि पहुचां सकते हैं।

• **सॉफ्टवेयर पाइरेसी**– सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है। इससे सॉफ्टवेयर कमपनियों को भारी नुकसान उठाना पड़ता है। साथ ही साथ इसके कीमती उपकरण भी ठीक से काम नहीं करते हैं।

• **फर्जी बैंक काल–** आपको जाली ईमेल, मसेज या फोन कॉल प्राप्त हो जो आपको बैंक जैसी लगे जिसमें आपसे पूछा जाये कि आपका एटीएम नम्बर और पासवर्ड की आवश्यकता है और यदि आपके द्वारा यह जानकारी नहीं दी गयी तो आपका खाता बंद कर दिया जायेगा या इस लिंक पर सूचना दें। याद रखें किसी भी बैंक द्वारा ऐसी जानकारी कभी भी इस तरह से नहीं मांगी जाती है और भूलकर भी अपनी किसी भी इस प्रकार की जानकारी को इन्टरनेट या फोनकॉल या मैसेज के माध्यम से नहीं बताये।

• **सोशल नेटवर्किंग साइटों पर अफवाह फैलाना**– बहुत से लोग सोशल नेटवर्किंग साइटों पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते हैं, लेकिन यूजर्स उनके इरादों को समझ नहीं पाते हैं और जाने–अनजाने में ऐसे लिक्सं को शेयर करते हैं, लेकिन यह भी साइबर अपराध और साइबर आतंकवाद की श्रेणी में आता है।

• **साइबर बुलिंग–** फेसबुक जैसी सोशल नेटवर्किंग 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। अकसर बच्चे इसका शिकार होते हैं।

सूचना तकनीक कानून, 2000 के अंतर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान

मानव समाज के विकास के नजरिये से सूचना और संचार तकनीकों की खोज को बीसवीं शताब्दी का सबसे महत्वपूर्ण आविष्कार माना जा सकता है। सामाजिक विकास के विभिन्न क्षेत्रों, खासकर न्यायिक प्रक्रिया में इस्तेमाल की महत्ता को कम करके नहीं आंका जा सकता, क्योंकि इसकी तेज गति, कई छोटी–मोटी दिक्कतों से छुटकारा, मानवीय गलतियों 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, जहां सभी संबंद्ध पक्षों की शारीरिक उपस्थिति अनिवार्य न हो, यह सर्वश्रेष्ठ विकल्प सिद्ध हो सकता है। सूचना तकनीक कानून के अंतर्गत उल्लिखित आरोपों की सूची निम्नवत हैः

• कंप्यूटर संसाधनों से छेड़छाड़ की कोशिश–धारा 65।

• कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश– धारा 66।

• संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान – धारा 66ए।

• कंप्यूटर या अन्य किसी इलैक्ट्रानिक गैजेट से चोरी की गई सूचनाओं को गलत तरीके से हासिल करने के लिए दंड का प्रावधान–धारा 66 बी।

• किसी की पहचान चोरी करने के लिए दंड का प्रावधान– धारा 66सी।

• अपनी पहचान छुपाकर कंप्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुंच बनाने के लिए दंड का प्रावधान– धारा 66डी।

• किसी की निजता भंग करने के लिए दंड का प्रावधान –धारा 66इ।

• साइबर आतंकवाद के लिए दंड का प्रावधान–धारा 66एफ।

• आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े प्रावधन–धारा 67।

• इलेक्ट्रानिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चो को अश्लील अवस्था में दिखाया गया हो–धारा 67बी।

• मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दंड का प्रावधान–धारा 67सी।

• सुरक्षित कंप्यूटर तक अनाधिकार पहुंच बनाने से संबंधित प्रावधान–धारा 70

• डाटा या आंकडों को गलत तरीके से पेश करना–धारा 71।

• आपसी विश्वास और निजता को भंग करने से संबंधित प्रावधान–धारा 72ए।

• कान्ट्रैक्ट की शर्तों का उल्लघंन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान–धारा 72ए।

• फर्जी डिजिटल हस्ताक्षर का प्रकाशन–धारा 73।

• सूचना तकनीक कानून की धारा 78 में इंस्पेक्टर स्तर के पुलिस अधिकारी को इन मामलों में जांच का अधिकार हासिल है।

भारतीय दंड संहिता में साइबर अपराधों से संबंधित प्रावधान –

• ईमेल के माध्यम से धमकी भरे संदेश भेजना– आईपीसी की धारा 503।

• ईमेल के माध्यम से ऐसे संदेश भेजना, जिससे मानहानि होती हो– आईपीसी की धारा 499।

• फर्जी इलैक्ट्रानिक रिकाडर्स का इस्तेमाल– आईपीसी की धारा 463।

• फर्जी वेबसाइटस या साइबर फॉड–आईपीसी की धारा 420।

• चोरी छुपे किसी के ईमेल पर नजर रखना– आईपीसी की धारा 463।

• वेब जैकिंग– आईपीसी की धारा 383।

• ईमेल का गलत इस्तेमाल– आईपीसी की धारा 500।

• दवाओं को ऑनलाइन बेचना– एनडीपीएस एक्ट।

• हथियारों की ऑनलाइन खरीद बिक्री– आर्म्स एक्ट।

साइबर आतंकवाद के लिए दंड का प्रावधान–

साइबर आतंकवाद के मामलों में दंड विधान के लिए सूचना तकनीक कानून, 2000 में धारा 66–एफ को जगह दी गई है।

1– यदि कोई–

अ– भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को भंग करने या इसके निवासियों को आतंकित करने के लिए।

क– किसी अधिकृत व्यक्ति को कंप्यूटर के इस्तेमाल से रोकता है या रोकने का कारण बनता है।

ख– बिना अधिकार के या अपने अधिकार का अतिक्रमण कर जबरन किसी कंप्यूटर के इस्तेमाल की कोशिश करता है।

ग– कंप्यूटर में वायरस जैसी कोई ऐसी चीज डालता है या डालने की कोशिश करता है, जिससे लोगों की जान को खतरा पैदा होने की आंशका हो या संपत्ति के नुकसान का खतरा हो या जीवन के लिए आवश्यक सेवाओं में जानबूझ कर खलल डालने की कोशिश करता हो या धारा 70 के तहत संवेदनशील जानकारियों पर बुरा असर पड़ने की आशंका हो या–

आ– अनाधिकार या अधिकारों का अतिक्रमण करते हुए जानबूझ कर किसी कंप्यूटर से ऐसी सूचनाएं हासिल करने में कामयाब होता है, जो देश या सुरक्षा या अन्य देशों के साथ उसके संबंधों के नजरियें से संवेदनशील है या कोई भी गोपनीय सूचना इस इरादें के साथ हासिल करता है, जिससे भारत की सुरक्षा, एकता, अखंडता एवं संप्रभुता, अन्य देशों के साथ इसके संबंध, सार्वजनिक जीवन या नैतिकता पर बुरा असर पड़ता हो या ऐसा होने की आशंका हो, देश की अदालतों की अवमानना अथवा मानहानि होती हो या ऐसा होने की आशंका हो, किसी अपराध को बढ़ावा मिलता हो या इसकी आशंका हो, किसी विदेशी राष्ट्र अथवा व्यक्तियों के समूह अथवा किसी अन्य को ऐसी सूचना से फायदा पहुंचता हो, तो उसे साइबर आतंकवाद का आरोपी माना जा सकता है।

2– यदि कोई व्यक्ति साइबर आतंकवाद फैलाता है या ऐसा करने की किसी साजिशों में शामिल होता है तो उसे आजीवन कारावास की सजा सुनाई जा सकती है।

2005 में प्रकाशित एडवास्ंड लॉ लेक्सिकॉन के तीसरे संस्करण में साइबर स्पेस शब्द को भी इसी तर्ज पर परिभाषित किया गया है। इसमें इलैक्ट्रानिक माध्यमों में फलोटिंग शब्द पर खासा जोर दिया गया है, क्योंकि दुनिया के किसी भी हिस्से से इस तक पहुंच बनाई जा सकती है। लेखक ने आगे इसमें साइबर थेफ्ट शब्द को ऑनलाइन कंप्यूटर सेवाओं के इस्तेमाल के परिप्रेक्ष्य में परिभाषित किया है। इस शब्दकोष में साइबर कानून की इस तरह व्याख्या की है, कानून का वह क्षेत्र, जो कंप्यूटर और इंटरनेट से संबंधित है और उसके दायरे में इंटेलेक्चुअल

प्रॉपर्टी राइटस, अभिव्यक्ति की स्वतंत्रता और सूचनाओं तक निर्बाध पहुंच आदि आते हैं।

सूचना तकनीक कानून में कुछ और चीजों को परिभाषित किया गया है, जो इस प्रकार हैं, कंप्यूटर से तात्पर्य किसी भी ऐसे इलेक्ट्रानिक, मैग्नेटिक, आप्टिकल या तेज गति से डाटा का आदान–प्रदान करने वाली किसी भी ऐसे यंत्र से है, जो विभिन्न तकनीकों की मदद से गणितीय, तार्किक या संग्रहणीय कार्य करने में सक्षम है। इसमें किसी कंप्यूटर तंत्र से जुड़ा या संबंधित हर प्रोग्राम और साफ्टवेयर शामिल है।

सूचना तकनीक कानून, 2000 की धारा 1 (2) के अनुसार, उल्लिखित अपवादों को छोड़कर इस कानून के प्रावधान पूरे देश में प्रभावी हैं। साथ ही उपरोक्त उल्लिखित प्रावधानों के अंतर्गत देशी की सीमा से बाहर किए गए किसी अपराध की हालत में भी उक्त प्रावधान प्रभावी होंगे।

संदर्भ ग्रंथ

1. तलफ फातिमा, इंटरनेट विधि एवं साइबर अपराध।
2. राय हाकिम, साइबर क्राइम।
3. देवारती हालदर, के0 जयशंकर, भारत में महिलाओं के विरूद्ध साइबर अपराध।
4. एड0 प्रशांत माली, साइबर कानून और साइबर अपराध।