साइबर अपराध या कंप्यूटर उन्मुखी अपराध

'डिजिटल दुनिया ऐसी परिस्थितियों का निर्माण करती है जहाँ कुछ भी गोपनीय या रहस्य नहीं रह जाता।'

कितनी सत्य है उपर्युक्त पंक्तियाँ? वर्तमान विश्व क्या सच में ऐसी स्थिति में पहुँच गया है जहाँ कुछ भी छुपा हुआ नहीं है? अगर गौर से देखा जाए तो हाँ, बहुत हद तक आज यह स्थिति आ गयी है। इंटरनेट ने समूचे विश्व की सीमाओं को लांघकर ज्ञान, सूचना और संपर्क संबंधी क्रांति को सभी व्यक्तियों तक उपलब्ध कराया है। गौरतलब है कि ज्ञान और अभिव्यक्ति के विस्तार से सुविधाओं में भी विस्तार हुआ है लेकिन विकृत मानसिकताओं के चलते इस व्यवस्था के दुरूपयोग संबंधी मामले आए दिन सामने आ रहे हैं। वर्तमान में, प्राय: अंतर्राष्ट्रीय स्तर के सभी सम्मेलनों में साइबर क्राइम चर्चा का विषय बन चुका है।

आज के समय में इंटरनेट समय-बचत का सबसे बड़ा माध्यम बन गया है क्योंकि किसी भी कार्य को करने हेतु लगने वाला खर्च आधे से भी कम रह गया है। इंटरनेट ने हमारी जिंदगी को अनुशासन, सलीका और सुनिश्चितता प्रदान की है, लेकिन इसके साथ-साथ इंटरनेट पर आज अपराध का एक समृद्ध संसार फल-फूल रहा है। इस आपराधिक संसार के ट्रोलिंग, सूचना एवं पहचान की चोरी, यौन अपराध, पोर्नोग्राफी, वायरस अटैक आदि मुख्य अवयव हैं।

साइबर अपराधों को दो तरह से वर्गीकृत किया जा सकता है-

1. **एक लक्ष्य के रूप में कंप्यूटर** (अन्य कंप्यूटरों पर आक्रमण करने के लिये एक कंप्यूटर का उपयोग) जैसे कि हैकिंग, वायरस आक्रमण, DOS आक्रमण आदि।
2. **एक शस्त्र के रूप में कंप्यूटर** अर्थात्, साइबर आतंकवाद, बौद्धिक संपदा अधिकारों के उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, अश्लीलता का प्रसार इत्यादि।

साइबर क्राइम एक ऐसा गैर-कानूनी कार्य होता है जिसमें सूचना तकनीक या कंप्यूटर का उपयोग किया जाता है। सूचना तकनीकी में हुयी प्रगति ने आपराधिक गतिविधियों के क्षेत्र में नई संभावनाओं का मार्ग भी खोला है। इस प्रकार के अपराधों से निपटने हेतु साइबर कानून भी बनाए गए हैं।

साइबर क्राइम के तहत आने वाले विभिन्न कार्य:-

- **अनधिकृत पहुँच और हैकिंग:**
  किसी भी कंप्यूटर या कंप्यूटर नेटवर्क में बिना अनुमति प्रवेश करने को अनधिकृत पहुँच बनाना या हैकिंग कहते हैं। इस प्रकार के कार्य आमतौर पर वित्तीय अपराधों के संदर्भ में देखे जाते हैं। कुछ उदाहरण निम्न हैं-
  - किसी बैंक के खाताधारकों के अकाउंट से दूसरे अकाउंट में पैसे स्थानांतरित करना।
  - किसी व्यक्ति के क्रेडिट कार्ड की जानकारी चुरा कर उसका दुरूपयोग करना।
  - किसी वेबसाइट के घटक को अनधिकृत तरीके से परिवर्तित करना।

भारत के संदर्भ में हैकिंग संबंधित कार्यविधियों को गैरकानूनी दर्जा प्राप्त है एवं इनफॉर्मेशन टेक्नोलॉजी एक्ट, 2008 के तहत सजा का प्रावधान है।

- **डाटा चोरी:**
  किसी संस्था या व्यक्ति या कंप्यूटर नेटवर्क में अनधिकृत व्यक्ति द्वारा बिना अनुमति लिये उसके कंप्यूटर के डाटा की कॉपी करना या उसे साझा करना डाटा चोरी अपराध के तहत माना जाता है।
- **कंप्यूटर वायरस का प्रसार:**
  किसी प्रोग्राम को किसी कंप्यूटर या कंप्यूटर नेटवर्क की अनुमति के बिना कंप्यूटर में प्रवेश कराना, कंप्यूटर वायरस को फैलाने की श्रेणी में आता है। आमतौर पर वायरस प्रोग्राम का कार्य किसी अन्य के कंप्यूटर डाटा को खराब करना होता है। जैसे कि किसी विमान सेवा के कंप्यूटर में वायरस के प्रवेश द्वारा डाटा के बदलने से प्लेन के दुर्घटनाग्रस्त होने की संभावना बन सकती है।
- **पहचान की चोरी:**
  किसी अन्य व्यक्ति की पहचान चुराकर कंप्यूटर नेटवर्क पर कार्य करना इस अपराध की श्रेणी में आता है या फिर कंप्यूटर नेटवर्क पर स्वयं की पहचान छुपाते हुए स्वयं को दूसरे के नाम से उजागर करते हुए उस व्यक्ति के नाम पर धोखाधड़ी या घपला करना।
- **ट्रोजन हमला:**
  ट्रोजन प्रोग्राम वैसे प्रोग्राम होते हैं जो देखने में उपयोगी लगते हैं लेकिन उनके द्वारा कंप्यूटर या कंप्यूटर नेटवर्क को नुकसान पहुँचाया जाता है।

इस प्रकार साइबर अपराध के अंतर्गत ऐसे गैर-कानूनी कार्यों को सम्मिलित किया जाता है, जिनसे कंप्यूटर प्रणाली को हथियार के रूप में इस्तेमाल करके अन्य

कंप्यूटरों को निशाना बनाया जाता है। वर्तमान में साइबर अपराध के जरिये सोशल नेटवर्किंग के माध्यम से किसी व्यक्ति की निजता में अनधिकार प्रवेश के अतिरिक्त उसकी गोपनीय सूचनाओं की जानकारी को साझा करके उससे धन की उगाही की जाती है। साइबर युद्ध के माध्यम से एक देश दूसरे देश के कंप्यूटर नेटवर्क को नष्ट कर देता है अथवा सामरिक दृष्टि से महत्त्वपूर्ण जानकारियों को हासिल करके राष्ट्र की संप्रभुता को चुनौती देता है। अमेरिका तथा इजरायल ने जहां वर्ष 2009 में ईरान के परमाणु कार्यक्रम के खिलाफ साइबर तकनीक का इस्तेमाल किया था तो वहीं 2016 में संपन्न हुए अमेरिकी राष्ट्रपति चुनाव में रूसी सरकार द्वारा हैकिंग की बात सामने आयी थी। हैकिंग का वह बहुचर्चित मामला संपूर्ण विश्व के लिये एक चेतावनी का विषय बन कर उभरा था। वैसे इस समस्या पर अंकुश लगा पाना किसी एक देश के बस की बात नहीं है। यह एक वैश्विक समस्या है और इसका समाधान भी वैश्विक स्तर पर ही तलाशा जा सकता है।

विचारणीय बिंदु यह है कि भारत अपनी विविधता के कारण इस तरह के हमलों के लिये एक मुफीद जगह बन कर उभरा है। भारत में साइबर सुरक्षा तंत्र का विकास अभी अपनी प्रारंभिक अवस्था में है। ऐसे समय में जहाँ हमारा देश 'डिजिटलीकरण' की ओर तेजी से बढ़ रहा है, साइबर सुरक्षा का खतरा भी बढ़ता जा रहा है। भारत में इंटरनेट पर निज़ता के हनन की समस्या भी गंभीर होती जा रही है। 'रैनसमवेयर' जैसे कंप्यूटर वायरस का भारत सहित दुनिया के देशों पर हुए हमले को संभवत: आजतक के इतिहास का सबसे बड़ा साइबर हमला माना जाता है।

अत: वर्तमान डिजिटल एवं सूचना-संचार तकनीकी के युग में, जबकि इंटरनेट का अत्यधिक प्रयोग बढ़ता जा रहा है, इन परिस्थितियों में एक बेहतर 'साइबर सुरक्षा' की आवश्यकता है। साइबर सुरक्षा का तात्पर्य साइबर स्पेस की हमले, क्षति, दुरुपयोग आदि आर्थिक जासूसी से सुरक्षित करना है। साइबर अपराधों के बढ़ते हुए वैविध्य तथा गहनता को देखते हुए सभी राष्ट्रों को मिल जुलकर इस समस्या के समाधान की ओर अग्रसर होने का प्रयास करना चाहिये, क्योंकि वैश्वीकरण सूचना एवं संचार तकनीकी के युग में सभी राष्ट्रों के समन्वित प्रयासों से ही इस समस्या का समुचित समाधान निकाला जा सकता है। इसी दिशा में 2004 में 'बुडापेस्ट' से अवांछित साइबर गतिविधियों पर रोक के लिये एक सम्मेलन का आयोजन किया गया। इस सम्मेलन का मुख्य उद्देश्य साइबर अपराध से समाज को सुरक्षा उपलब्ध कराए जाने के लिये एक सामान्य नीति बनाना था। इसमें कुछ विशेष शक्तियों और प्रक्रियाओं का उल्लेख है, जिनमें हानिकारक कंप्यूटर नेटवर्क की खोज तथा उन पर रोक शामिल है। भारत में भी साइबर हमलों की बढ़ती संख्या को देखते हुए समय-समय पर इस दिशा में प्रयास किये गए हैं, जैसे- सूचना प्रौद्योगिकी (संशोधन) अधिनियम-2008 भारत की नई साइबर नीति-2013, सूचना प्रौद्योगिकी विभाग द्वारा साइबर सुरक्षा के लिये एक संस्थान 'सर्ट इन' इत्यादि का प्रावधान किया गया है।

डिजिटल होती दुनिया में साइबर अपराध एक गंभीर एवं जटिल समस्या है। हैकरों द्वारा प्राय: उन्हीं कंप्यूटर नेटवर्कों में सेंध लगायी जाती है जिनका सुरक्षा-नेटवर्क कमजोर होता है। अत: तकनीक को उन्नत करते हुए तकनीकी रूप से सुदृढ़ नेटवर्क का निर्माण करना हमारी प्राथमिक आवश्यकता होनी चाहिए। इसके लिये आईटी तकनीकों, बायोमेट्रिक तकनीक प्रणाली इत्यादि का उपयोग करके साइबर अपराधों को रोका जा सकता है। साइबर सुरक्षा के आर्थिक पक्ष के तहत 'साइबर बीमा' एक बेहतर प्रयास हो सकता है।

आज जबकि इंटरनेट क्रांति अपनी पाँचवीं पीढ़ी में प्रवेश कर गई है तो ऐसे में यदि हमने साइबर हमलों की चुनौती को पार कर इंटरनेट को सुरक्षित एवं भरोसेमंद बनाने में सफलता प्राप्त कर ली तो अवश्य ही सूचना की यह क्रांति हमारे लिये वरदान सिद्ध होगी।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/cybercrime-or-computer-oriented-crime