ARYAVART SHODH VIKAS PATRIKA
RNI TITLED NO. UPBIL04292
RNI REG. NO. UPBIL/2014/66218 PP. No.- 148-153

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- I, Issues-27, YEAR- Jan.-March-2023

भारत में साइबर अपराध एवं उससे सम्बन्धित कानून

डॉ0 शैलेन्द्र कुमार सिंह

एसोसिएट प्रोफेसर– समाजशास्त्र विभाग, बैसवारा पी०जी० कालेज, लालगंज, रायबरेली (उ0प्र0) भारत

Received-14.01.2023, Revised-20.01.2023, Accepted-26.01.2023 E-mail: drsksinghbdc@gmail.com

सारांशः ***इन्टरनेट के जन्म और विकास के साथ ही साइबर अपराध की उत्पत्ति हुयी। दुनिया में सबसे अधिक इन्टरनेट उपयोगकर्ता लगभग 80 करोड़ भारत में हैं। इन्टरनेट उपयोगकर्ताओं में वृद्धि के साथ–साथ साइबर अपराधों में भी वृद्धि हुई है। नेशनल क्राइम रिकार्ड ब्यूरो के अनुसार देश में साइबर अपराधों की संख्या वर्ष 2010 में 966 थी जो वर्ष 2019 में बढ़कर 44735, वर्ष 2020 में 50035 तथा वर्ष 2021 में 52974 हो गयी। भारतीय रिजर्व बैंक के अनुसार वित्तीय वर्ष 2019–2020 में 185 करोड़ रुपये की एवं वित्तीय वर्ष 2020–2021 में 165 करोड़ रुपये की धोखाधड़ी हुयी। साइबर अपराध पर नियन्त्रण हेतु भारतीय सूचना प्रौद्योगिकी अधिनियम सन् 2000 में पारित किया गया। सरकार द्वारा वर्ष 2013 में राष्ट्रीय साइबर सुरक्षा नीति जारी की गयी एवं वर्ष 2019 में राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल की स्थापना की गयी।***

कुंजीभूत शब्द– इन्टरनेट, साइबर अपराध, नेशनल क्राइम रिकार्ड ब्यूरो, भारतीय रिजर्व बैंक, भारतीय सूचना प्रौद्योगिकी।

इक्कीसवीं सदी में मनुष्य को इन्टरनेट ने सर्वाधिक प्रभावित किया है। यह मनोरंजन, शिक्षा, व्यापार का महत्वपूर्ण साधन है। आज इन्टरनेट से सारी दुनिया एक वैश्विक गाँव हो गयी है। साइबर शब्द की उत्पत्ति विलियम गिब्सन जो काल्पनिक विज्ञान कथाएँ लिखते थे, की 1948 में प्रकाशित पुस्तक न्यूरान एन्सर में वर्णित साइबर स्पेस शब्द से हुआ। आज साइबर स्पेस का अर्थ इन्टरनेट के रूप में समझे जाने वाले वैश्विक कम्प्यूटर तन्त्र (नेटवर्क) से है। इन्टरनेट का उद्भव एवं विकास अमेरिका के प्रतिरक्षा विभाग के मुख्यालय पेंटागन स्थित 'एडवांस्ड रिसर्च प्रोजेक्ट्स एजेन्सी–एरपा (ARPA) की संकल्पना से सन् 1969 ई0 में हुआ था। इन्टरनेट आप्टिकल फाइबर तारों से जुड़े कम्प्यूटरों का एक व्यापक नेटवर्क है। भारत में इन्टरनेट का प्रवेश 1987–1988 में हो चुका था, किन्तु विदेश संचार निगम लिमिटेड द्वारा इण्टरनेट सुविधा को जनसामान्य को उपलब्ध कराने के उद्देश्य से 15 अगस्त 1995 को 'गेटवे इन्टरनेट' सेवा आरम्भ की गयी। 1995 में ही मोबाइल फोन सेवा की शुरूआत हुई। सन् 2009 में 3जी टेक्नॉलोजी एवं सन् 2012 में 4जी टेक्नॉलोजी ने मोबाइल पर तीव्र इन्टरनेट उपलब्ध कर दिया। इंटरनेट के जन्म और विकास के साथ ही साइबर अपराध की उत्पत्ति हुई। कम्प्यूटर वैज्ञानिक जेवियर गीज के अनुसार ''साइबर अपराध कम्प्यूटर और इन्टरनेट के माध्यम से होने वाला अपराध है जिसके अन्तर्गत जालसाजी, अनाधिकृत प्रवेश, चाइल्ड पोर्नोग्राफी और साइबर स्टॉकिंग शामिल है।'' संयुक्त राष्ट्र के कम्प्यूटर क्राइम कन्ट्रोल एण्ड प्रिवेंशन मैनुअल के अनुसार जालसाजी, ठगी और अनाधिकृत प्रवेश को ही साइबर अपराध की परिभाषा में शामिल किया गया है।

साइबर अपराध के प्रकार–

प्रमुख साइबर अपराध निम्नलिखित हैं:–

1. हैकिंग
2. साफ्टवेयर पायरेसी
3. वायरस
4. साइबर स्क्वैटिंग
5. साइबर स्टॉकिंग
6. बौद्धिक सम्पदा की चोरी
7. साइबर गैम्बलिंग
8. साइबर डिफेमेशन
9. पोर्नोग्राफी
10. फिसिंग
11. नाइजीनियन स्कैम

हैकिंग– हैकिंग से तात्पर्य किसी कम्प्यूटर सिस्टम या नेटवर्क में प्रवेश करके किसी व्यक्ति या संस्था के डाटा को चुराना या अनाधिकृत प्रवेश करना है। एन0आई0सी0 भारतीय मिलिटरी अकादमी समेत कई प्रमुख संस्थाओं की साइट वर्ष 2007 में हैक की गयी।

हैकर्स कम्प्यूटर तकनीक के विशेषज्ञ होते हैं जो नेटवर्क में अनाधिकृत रूप में प्रवेश कर जाते हैं। हैकिंग के जरिये आर्थिक गतिविधियों को भी प्रभावित करते हैं। मार्च, 2000 में क्यूरेडर नाम के हैकर ने अमेरिका, कनाडा, थाईलैण्ड, जापान

अनुरूपी लेखक/संयुक्त लेखक

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- I, Issues-27, YEAR- Jan.-March-2023

और ब्रिटेन से काम करने वाली ई–कामर्स वेबसाइट से 28000 क्रेडिट कार्ड्स के नम्बर उड़ा लिये। बहुत से हैकर्स विभिन्न कम्पनियों के डाटा चुराकर उन्हें प्रतिद्वन्दी कम्पनियों को भारी कीमत पर बेचते हैं।

साफ्टवेयर पायरेसी– किसी कम्पनी के साफ्टवेयर की नकली कापी बनाकर बेचना या उस कम्पनी को उसके साफ्टवेयर को क्रय किये बिना ही उसका उपयोग करना साफ्टवेयर पायरेसी कहलाता है। भारत में आज भी कुल प्रयोग किये जाने वाले साफ्टवेयर का 60% पायरेटेड होता है।

वायरस– वायरस एक प्रकार का साफ्टवेयर प्रोग्राम होता है जो कम्प्यूटर को नुकसान पहुंचाता है। मेलीसा वायरस के कारण पूरी दुनिया के दस लाख से ज्यादा कम्प्यूटर को नुकसान हुआ था। जून 2005 में माइकल जैक्सन की आत्महत्या के खबर के साथ एक वायरस आया जो कम्प्यूटर में एकत्रित जानकारी चुरा लेता था। वर्ष 2020 में लगभग 82% भारतीय कम्पनियों को रैनसमवेयर हमलों का सामना करना पड़ा।

साइबर स्क्वैटिंग– इसके अन्तर्गत किसी स्थापित कम्पनी के नाम को चुरा लिया जाता है।

साइबर स्टाकिंग– किसी व्यक्ति को अवाँछित सूचनायें भेजकर आतंकित या परेशान करने को साइबर स्टाकिंग कहा जाता है। इसमें अपराधी अधिकतर पुरुष तथा पीड़ित अधिकतर महिलायें होती हैं। साइबर स्टाकिंग एक व्यक्ति को मनोवैज्ञानिक रूप से परेशान करता है।

बौद्धिक सम्पदा की चोरी– बौद्धिक सम्पदा को एक नवाचार, नए शोध माडल के रूप में परिभाषित किया गया है जिसका आर्थिक मूल्य है। बौद्धिक सम्पदा का लोग पेटेन्ट कराने के साथ संगीत का कापीराइट सुरक्षित रखते हैं। जब कोई व्यक्ति कापीराइट वाली चीज को अपने नाम से पेटेन्ट करवा लेता है तो वह बौद्धिक सम्पदा की चोरी कहलाता है।

साइबर गैम्बलिंग– इसमें इन्टरनेट के माध्यम से गैम्बलिंग (जुआखोरी) की जाती है। आनलाइन लाटरी में लोगों को आकर्षित करने का प्रयास किया जाता है। इसमें पोकर, स्पोर्ट गेम, कैसिनो गेम आदि हैं।

साइबर डिफेमेशन या वेब डिफेमेण्ट– इसमें किसी व्यक्ति द्वारा अन्य किसी इन्टरनेट उपयोगकर्ता का पासवर्ड तोड़कर उसके नाम से दूसरे व्यक्ति (सगे–सम्बन्धी, दोस्त) को बदनाम करने वाली ई–मेल भेजी जाती है जिसकी जानकारी उपयोगकर्ता को नहीं हो पाती है और बाद में जिसके पास ई–मेल पहुंचती है वह उससे वाद–विवाद करता है।

पोर्नोग्राफी– पोर्नोग्राफी का अर्थ नग्न चित्रण है। इसके अन्तर्गत अश्लील चित्रों एवं फिल्मों का प्रसार किया जाता है।

साइबर बुलिंग– साइबर बुलिंग से तात्पर्य ई–मेल, एस0एम0एस0, व्हाट्सऐप या सोशल मीडिया के माध्यम से किसी व्यक्ति को डराना, धमकाना या भयभीत करना है।

फिसिंग– यह गोपनीय सूचनाओं को प्राप्त करने का फर्जी तरीका है। इसमें चारा डालकर अर्थात् लालच दिखाकर लोगों को फंसाया जाता है। धन का लालच, इनकम टैक्स रिफण्ड, इंश्योरेन्स पोलिसी बोनस, लॉटरी आदि का लालच दिखाकर लोगों के साथ ठगी की जाती है।

नाइजीरियन स्कैम या एडवाँस फी फ्रॉड या 419 फ्रॉड– इन्टरनेट के माध्यम से लोगों को ई–मेल भेजकर अधिक धन प्राप्त करने का लालच दिया जाता है। अधिक धन प्राप्त करने के लालच में लोग छोटी राशि देने को तैयार हो जाते हैं। नाइजीरिया में इस तरह के अपराधों की उत्पत्ति हुई और धीरे–धीरे यह दुनिया के अन्य भागों में भी पहुँच गये। नाइजिरियाई कानूनी कोड की धारा–419 इसे प्रतिबन्धित करती है। इसीलिये इस स्कैम को 419 फ्रॉड के नाम से भी जाना जाता है।

साइबर स्क्वेटिंग– साइबर स्क्वेटिंग का मतलब है कि प्रसिद्ध संस्था के नाम की साइट का रजिस्ट्रेशन इस आशय से कराना कि भविष्य में इसे मंहगे दाम पर बेचा जायेगा। 1990 के दशक के अन्त में साइबर स्क्वेटिंग का खतरा उठाया गया था। साइबर स्क्वेटिंग के शुरूआती पीड़ितों में पैनासोनिक, हर्ट्ज, एवन आदि शामिल थे। वर्तमान में भारत में कोई कानून प्रभावी नहीं है जो साइबर स्क्वाटिंग के मुद्दे को सम्बोधित करता हो।

भारत में साइबर अपराध– दुनिया में सबसे अधिक इन्टरनेट उपयोगकर्ता लगभग 80 करोड़ लोग भारत में हैं। इन्टरनेट उपयोगकर्ताओं की संख्या में वृद्धि के साथ–साथ साइबर अपराधों में भी वृद्धि हो रही है। नेशनल क्राइम रिकॉर्ड ब्यूरो के अनुसार देश में साइबर अपराधों की संख्या वर्ष 2010 में 966 थी जो वर्ष 2019 में बढ़कर 44735, वर्ष 2020 में 50,035 तथा वर्ष 2021 में 52974 हो गई। एन0सी0आर0बी0 (NCRB) के अनुसार साइबर अपराध के मामलों में चार्जशीट फाइल होने वाले मामलों की संख्या 33.8 प्रतिशत रही, जबकि एक तिहाई मामलों में ही पुलिस जांच पूरी हो सकी। वर्ष 2021 में राज्यों और केन्द्र शासित प्रदेशों में सबसे ज्यादा साइबर अपराध तेलंगाना में 10,303 दर्ज हुए। इसके बाद उत्तर प्रदेश में 8829, कर्नाटक में 8136, महाराष्ट्र में 5562 दर्ज हुये।

मई 2017 में दुनियाभर के कई देशों में वानाक्राई रैनसमवेयर का हमला हुआ, जिसमें 2 लाख से ज्यादा कम्प्यूटर सिस्टम प्रभावित हुये। भारत भी इसमें शामिल था।

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- I, Issues-27, YEAR- Jan.-March-2023

मार्च, 2018 में हरियाणा बिजली वितरण निगम के पंचकुला स्थित हेड ऑफिस के कम्प्यूटर पर एक मैसेज भेजा गया जिसमें लिखा था कि आपका सिस्टम हैक हो चुका है। इसके बदले में 1 करोड़ रुपये की मांग की गयी थी जिसे बिटकॉइन में जमा करना था। अप्रैल, 2019 में तेलंगाना और आन्ध्र प्रदेश स्टेट पावर यूटिलिटी पर रैनसमवेयर हमला हुआ। इससे इनके सिस्टम पर हैकर्स का कन्ट्रोल हो गया और कई तरह की सर्विसेज प्रभावित हुई।

2019 में इंडियन बेस्ड हेल्थ सर्विस वेबसाइटें साइबर हमले का शिकार हुई थीं। इसमें हैकर ने मरीजों के साथ–साथ डॉक्टरों के भी 68 लाख रिकार्ड चुरा लिये थे।

स्कैमर्स ने 2018 में पूणे की कासमॉस बैंक पर अटैक किया था। इस साइबर हमले में हैकर्स ने कासमॉस कोआपरेटिव बैंक लिमिटेड से 94.42 करोड़ रुपये कि चोरी की थी। हैकर्स ने पहले तो बैंक के ए0टी0एम0 सर्वर को हैक कर कई वीजा और रुपया डेबिट कार्ड धारकों की जानकारी हासिल की और फिर उनके रुपये चुरा लिये। वर्ष 2018 के आरम्भ में ही स्कैमर्स ने 1.1 बिलियन भारतीयों का आधार कार्ड धारकों के डाटा की चोरी कर ली थी। इस डेटा में आधार, पैन और मोबाइल नम्बर, बैंक खाता नम्बर, आई0एफ0एस0सी0 कोड और कार्डधारकों की व्यक्तिगत जानकारी शामिल थी।

मुम्बई के दो हैकर्स को अगस्त, 2018 में कई बैंक खातों से अवैध रूप से 4 करोड़ रुपये ट्रान्सफर करने के आरोप में गिरफ्तार किया गया था।

भारतीय रिजर्व बैंक के अनुसार, वित्तीय वर्ष 2019–20 में 185 करोड़ रुपये की एवं वित्तीय वर्ष 2020–21 में 160 करोड़ रुपये की धोखाधड़ी हुई। वित्तीय वर्ष 2021–22 में 17.5 प्रतिशत की गिरावट के साथ यह राशि 128 रुपये रह गई। 31 दिसम्बर, 2022 को हैकर्स ने अहमदाबाद के डेवलपर दुष्यन्त पटेल के फोन को हैक कर उनके खाते से सिर्फ 30 मिनट में 37 लाख रुपये चोरी कर लियें इसमें दुष्यन्त ने किसी से अपने बैंकिंग क्रेडेंशियल्स या ओ0टी0पी0 शेयर नहीं किया था।

सूचना एवं प्रसारण मंत्री अनुराग ठाकुर ने लोकसभा में बताया कि 2017 से अप्रैल, 2022 तक कुल 641 सरकार के ट्विटर हैंडल और ई–मेल अकाउन्ट हैक हुए हैं।

23 नवम्बर, 2022 को देश के सबसे बड़े अस्पताल अखिल भारतीय आयुर्विज्ञान संस्थान (AIIMS) दिल्ली के ऑनलाइन सिस्टम पर बड़ा साइबर हमला हुआ जिसमें करीब 4 करोड़ मरीजों का डाटा चोरी हुआ। यह देश के मेडिकल सेक्टर में अब तक की सबसे बड़ी हैकिंग हैं। पुलिस इसे रैनसमवेयर अटैक मान रही है। समाचार एजेन्सी पी.टी.ई. ने खुलाया किया कि हैकरों ने इस मामले में क्रिप्टोकरेन्सी में 200 करोड़ रुपये की मांग की। फार्मा कम्पनियां, सर्जिकल इंस्ट्रूमेन्ट कम्पनियाँ और अन्य मेडिकल एजेन्सियाँ इस डाटा का फायदा अपने हितों के लिये उठा सकती है।

इंडसफेस की हालिया रिपोर्ट के अनुसार भारत में हर महीने हेल्थ केयर सेक्टर पर लगभग 3 लाख साइबर हमले होते हैं। ये दुनियाभर में दूसरे सबसे अधिक साइबर हमले हैं।

सन् 2020 में कम से 130 अलग–अलग रैनसमवेयर एक्टिव थे। हमलावर अपने रैनसमवेयर को ज्यादा से ज्यादा लोगों तक पहुंचाने के लिये जाने–माने बॉटनेट मालवेयर और अन्य रिमोट एक्सेस ट्रोजन (RAT) सहित कई तरीकों का इस्तेमाल कर रहे हैं।

झारखण्ड राज्य का एक जिला जामताड़ा साइबर ठगी का गढ़ माना जाता है और ऐसा कहा जाता है कि पूरे देश में हो रही साइबर ठगी के 80 प्रतिशत मामले जामताड़ा से जुड़े हुए हैं। यहीं के साइबर ठगों द्वारा अमिताभ बच्चन के बैंक खाते से 5 लाख रुपये, पंजाब के मुख्यमंत्री अमरिन्दर सिंह की पत्नी और सांसद परणीत कौर के खाते से करीब 23 लाख रुपये गायब कर दिये थे। पुलिस की रिपोर्ट के अनुसार, जामताड़ा में साइबर ठगी की शुरूआत साल 2013 से हुई। उस समय से अब तक सैकड़ों साइबर अपराधियों को गिरफ्तार किया जा चुका है।

व्हाट्सएप का प्रयोग अधिकांश मोबाइल उपयोगकर्ता करते है। साइबर अपराधी वीडियोकॉल करके अश्लील वीडियो भेजते हैं, फोन कॉल उठाने वाले व्यक्ति की बात–चीत को रिकार्ड करके ब्लैकमेल करते हैं। जामताड़ा जगह इसके लिये कुख्यात है।

कौन बनेगा करोड़पति एक लोकप्रिय टी0वी0 शो है। लोगों को लाखों रुपये इनाम जीतने का झूठा संदेश भेजकर लोगों से ठगी की जाती है। देश में विगत कुछ वर्षों में ऑनलाइन कारोबार तेजी से बढ़ा है। कुछ अपराधी एक फ्त ब्यकम भेजते हैं जिसमें नीचे एक धनराशि लिखी होती है। जैसे ही लोग उसे स्कैन करते हैं, तो तुरन्त अकाउन्ट से पैसे कट जाते हैं। मुम्बई में एक साइबर धोखाधड़ी केस दर्ज किया, जिसमें डाक्टर ने ऑनलाइन अपनी बेटी के लिए 1200 रुपये की किताबें ऑर्डर की थी। इसके बाद डाक्टर को QR Code स्कैन करने के लिये कहा गया। फ्त ब्यकम स्कैन करने के बाद उसके अकाउन्ट से कुल 1,50,000 रुपये कट गये।

कई लोगों को झूठा एम0एस0एस0 भेजकर कि "यदि आज बिजली का बिल जमा नहीं किया, तो घर की बिजली कट

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- I, Issues-27, YEAR- Jan.-March-2023

जायेगी'' धोखाधड़ी की जा रही है। IIT में पढ़ने वाली एक लड़की को वर्क फ्रॉम होम के अन्तर्गत 9800 रुपये प्रतिदिन कमाने का झाँसा देकर उसके अकाउन्ट से 4 लाख रुपये निकाल लिये।

साइबर अपराध पर नियन्त्रण हेतु भारत के प्रयास– साइबर अपराध पर नियन्त्रण हेत भारतीय सूचना प्रौद्योगिकी अधि नियम सन् 2000 में पारित किया गया। देश में प्रथम साइबर क्राइम पुलिस स्टेशन की स्थापना सितम्बर, 2001 में कनार्टक राज्य के बंगलौर शहर में की गयी।

वर्ष 2004 में भारतीय कम्प्यूटर आपात प्रक्रिया दल ब्त्ज–पद (Indian Computer Emergency Response Team) की स्थापना की गई जो कि साइबर घटनाओं के बारे में सूचना एकत्रित करता है और उनका विश्लेषण व प्रचार करता है। वर्ष 2009 में राष्ट्रीय अपराध रिकार्ड ब्यूरो को अपराध एवं अपराधी ट्रैकिंग नेटवर्क एवं सिस्टम CCTNS परियोजना की मॉनीटरिंग, समन्वय एवं कार्यान्वय का कार्य सौंपा गया। यह परियोजना लगभग 15000 पुलिस स्टेशनों तथा देश के 5000 उच्च कार्यालयों को जोड़ती है।

वर्ष 2013 में सरकार द्वारा राष्ट्रीय साइबर सुरक्षा नीति जारी की गयी जिसके तहत सरकार द्वारा अति संवेदनशील सूचनाओं के संरक्षण हेतु राष्ट्रीय अति संवेदनशी सूचना अवसंरचना संरक्षण केन्द्र (NCIIPC) का गठन किया गया है। (National Critical Information Infrastructure Protection Centre&NCIIPC)

वर्ष 2015 में राष्ट्रीय साइबर समन्वय केन्द्र की स्थापना की गई, जो आसन्न और सम्भावित साइबर सुरक्षा खतरों के प्रति जागरूकता फैलाता है और सम्बन्धित संस्थाओं/सुरक्षा एजेन्सियों को समय रहते खतरों की रोकथाम की त्वरित कार्यवाही के लिये सचेत करता है और आवश्यक सूचनायें उपलब्ध कराता है।

वर्ष 2017 में ग्रह मंत्रालय के अन्तर्गत साइबर एवं सूचना सुरक्षा (C&IS) प्रभाव की स्थापना की गयी जिसका उद्देश्य है, साइबर सुरक्षा, साइबर अपराध, राष्ट्रीय सूचना सुरक्षा नीति एवं दिशा–निर्देश (NIESPG), नेट ग्रिड आदि के कार्यान्वयन से सम्बन्धित मामले देखता है।

वर्ष 2017 में इलेक्ट्रानिक्स और सूचना प्रौद्योगिकी मंत्रालय के द्वारा साइबर स्वच्छता केन्द्र (बॉटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेन्टर) की स्थापना की गई जो भारत में बॉटनेट संक्रमणों का पता लगाकर एक सुरक्षित साइबर स्पेस बनाने के लिए कार्य करता है। यह लोगों को उनके डाटा, कम्प्यूटर, मोबाइल फोन, घरेलू राउटर जैसे उपकरणों को सुरक्षित करने और मालवेयर संक्रमण को रोकने के लिए किये जाने वाले उपायों के प्रति जागरूक करता है। यह केन्द्र इन्टरनेट सेवा प्रदाताओं के साथ घनिष्ठ समन्वय और सहयोग से संचालित होता है और सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा–70बी के प्रावधानों के तहत भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया टीम (सीईआरटी–इन) द्वारा संचालित किया जा रहा है। भारत सरकार के गृह मंत्रालय द्वारा वर्ष 2019 में राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal&www.cybercrime.gov.in) की स्थापना की गई।

इस पोर्टल के माध्यम से कोई भी साइबर अपराधियों की शिकायत ऑनलाइन दर्ज करा सकता है। इस पोर्टल के माध्यम से केवल दिल्ली में वित्तीय साइबर अपराध के शिकार लोगों के लिये एक हेल्पलाइन शुरू की गयी है जो 155260 नम्बर पर या www.cybercrime.gov.in पर घटना की रिपोर्ट कर सकते हैं। वर्ष 2019 में रक्षा साइबर एजेन्सी की स्थापना की गई। साइबर जगत में सम्भावित खतरों से निपटने के लिये एकीकृत रक्षा स्टॉफ के तहत यह विशेष साइबर एजेन्सी गठित की गई है। केन्द्रीय गृह मंत्रालय वर्ष 2020 में जनता को साइबर अपराधों के प्रति जागरूक करने और सहायता प्रदान करने के लिये एक ट्विटर हैंडल 'साइबर दोस्त' की शुरूआत की है।

भारत में साइबर कानून– भारतीय सूचना प्रौद्योगिकी अधिनियम सन् 2000 में पारित किया गया। इससे पहले साइबर अपराधों को भारतीय दण्ड संहिता के अन्तर्गत ही दर्ज किया जाता था। भारत इस प्रकार का कानून बनाने वाला एशिया में सिंगापुर के बाद दूसरा राष्ट्र बन गया है। भारतीय सूचना प्रौद्योगिकी (संशोधन) अधिनियम–2008 एवं 2009 के अन्तर्गत कुछ नयी धारायें सम्मिलित की गयीं। इस एक्ट की प्रमुख धाराएँ निम्नलिखित हैं।

धारा 65– कम्प्यूटर स्त्रोत दस्तावेज के साथ छेड़छाड़ करना–इस धारा के अन्तर्गत कोई भी व्यक्ति जान–बूझकर कम्प्यूटर प्रोग्राम, कम्प्यूटर सिस्टम, कम्प्यूटर नेटवर्क के लिये प्रयुक्त स्त्रोत कोड को छिपायेगा, नष्ट करेगा या परिवर्तित करेगा तो वह इस धारा के अन्तर्गत साइबर अपराधी होगा। इसके अन्तर्गत अपराधी व्यक्ति को 3 वर्ष का कारावास या 2 लाख रुपये तक जुर्माना या दोनों का सजा का प्रावधान है।

धारा 66– हैकिंग– इस धारा के अन्तर्गत कोई भी व्यक्ति जान बूझकर कम्प्यूटर स्त्रोत में स्थित किसी सूचना को नष्ट करता है, हटाता या परिवर्तित करता है, तो वह हैकिंग का अपराधी है।

इसके अन्तर्गत अपराधी व्यक्ति को 3 वर्ष का कारावास या 2 लाख रुपये तक का जुर्माना या दोनों सजा का प्रावधान है।

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- I, Issues-27, YEAR- Jan.-March-2023

धारा 66क– इस धारा के अन्तर्गत यदि कोई व्यक्ति कम्प्यूटर के माध्यम से कोई झूठी सूचना, शत्रुता, घृणा या वैमनस्य फैलाने के प्रयोजन के लिये भेजता है, तो वह 3 वर्ष का कारावास और जुर्माने से दण्डनीय होगा।

धारा 66ख– यदि कोई व्यक्ति कम्प्यूटर संसाधन या संचार युक्ति बेईमानी से प्राप्त करेगा, तो तीन वर्ष के कारावास या एक लाख रुपये के जुर्माना या दोनों से दण्डित होगा।

धारा 66ग– यदि कोई व्यक्ति धोखाधड़ी से किसी अन्य व्यक्ति के डिजिटल हस्ताक्षर, पासवर्ड या किसी अन्य पहचान का प्रयोग करेगा, तो वह इस अपराध के लिये तीन वर्ष के कारावास या एक लाख रुपये के जुर्माने से दण्डित होगा।

धारा 66घ– यदि कोई व्यक्ति कम्प्यूटर संसाधन का प्रयोग करके प्रतिरूपण द्वारा छल करेगा तो इसके लिये तीन वर्ष के कारावास या एक लाख रुपये के जुर्माने से दण्डित होगा।

धारा 66ङ– यदि कोई व्यक्ति जान बूझकर किसी व्यक्ति के गुप्तांग का चित्र उसकी सहमति के बिना प्रकाशित या प्रसारित करेगा, तो उसे तीन वर्ष का कारावास या दो लाख रुपये के जुर्माना या दोनों से दण्डित किया जायेगा।

धारा 66च– के अनुसार यदि कोई व्यक्ति भारत की एकता, अखण्डता, सुरक्षा या प्रभुता को खतरे में डालने का कार्य इण्टरनेट के माध्यम से करेगा, तो इसे साइबर आतंकवाद का अपराध कहा जायेगा और इसके लिये आजीवन कारावास तक का दण्ड प्रदान किया जायेगा।

धारा 67– अश्लील सूचनाओं का प्रकाशन एवं विस्तारण– इसके अन्तर्गत कोई भी व्यक्ति अश्लील सामग्री को प्रेषित अथवा प्रकाशित करता है या इन्हें साकार रूप देता है तो उसे 5 वर्ष तक का कारावास अथवा 1 लाख रुपये तक जुर्माना अथवा दोनों सजा का प्रावधान है। ऐसा अपराध पुनः करने पर 10 साल का कारावास और 5 लाख का जुर्माना अथवा दोनों सजा का प्रावधान है।

धारा 72– के अनुसार जब कोई व्यक्ति किसी भी इलेक्ट्रॉनिक रिकार्ड, पत्राचार, सूचनाओं, प्रपत्रों को गैर कानूनी तरीके से पढ़ेगा या संचारित करेगा अथवा किसी भी ऐसी गतिविधि में संलग्न होगा तो उसे 2 वर्ष तक की कारावास अथवा 1 लाख रुपये जुर्माना या दोनों भी हो सकते हैं।

धारा 74– के अनुसार यदि कोई व्यक्ति जान–बूझकर धोखाधड़ी करने के उद्देश्य से किसी व्यक्ति के डिजिटल हस्ताक्षर को अन्य व्यक्तियों को उपलब्ध कराता है, तो उसे 2 वर्ष का कारावास अथवा 1 लाख रुपये जुर्माना या दोनों भी हो सकते हैं।

धारा 75– के अनुसार यह अधिनियम विदेशों में रहने वाले उन व्यक्तियों पर भी लागू होगा जिन्होंने भारत में कम्प्यूटर, कम्प्यूटर सिस्टम और नेटवर्क को क्षति पहुंचायी हैं।

धारा 76– के अनुसार इस अधिनियम के किसी प्रावधान नियम अथवा आदेशों के उल्लंघन की दशा में किसी कम्प्यूटर, कम्प्यूटर प्रणाली, फ्लॉपी, काम्पैक्ट डिस्क, पेन ड्राइव अथवा अन्य सहायक उपकरणों की जब्ती की जायेगी।

धारा 78– के अनुसार साइबर अपराध की विवेचना की जिम्मेदारी पुलिस उपाधीक्षक या उसके ऊपर के रैंक के अधिकारी को दी गयी है।

निष्कर्ष– आज देश में 80 करोड़ इन्टरनेट उपयोगकर्ता हैं, जो दुनिया में सर्वाधिक हैं। इन्टरनेट के आधुनिक युग में ऑनलाइन शिक्षा, व्यापार, ई–बैंकिंग, सोशल मीडिया का प्रचलन बढ़ा है। इसके साथ ही साइबर अपराध में भी तेजी से वृद्धि हुयी है। लोग अभी साइबर सुरक्षा के प्रति कम जागरूक हैं। सरकार द्वारा साइबर अपराधों को रोकने के लिए अखिल भारतीय सूचना प्रौद्योगिकी अधिनियम सन् 2000 में पारित किया गया, साथ ही विभिन्न संस्थाओं का गठन किया गया।

वर्तमान इन्टरनेट के युग में आवश्यक है कि सभी को साइबर सुरक्षा के प्रति जागरूक किया जाय। माध्यमिक एवं स्नातक स्तर पर इसे पाठ्यक्रम में सम्मिलित किया जाय। प्रत्येक जिले में साइबर थानों का गठन हो। पुलिस और जांच संस्थाओं में कम्प्यूटर शिक्षा प्राप्त प्रशिक्षित योग्य अधिकारी हों, जो साइबर अपराधों की जांच कर सकें। साइबर अपराधों की सुनवाई के लिये ई–अदालतों का गठन किया जाय, जिसमें न्यायाधीश व वकील भी कम्प्यूटर प्रौद्योगिकी के जानकार हों। साइबर अपराधी दुनिया में कहीं से भी अपराध कर सकते हैं। अतः अन्तर्राष्ट्रीय पुलिस या इन्टरपोल को भी अपनी महत्वपूर्ण भूमिका निभानी होगी। संयुक्त राष्ट्र संघ के माध्यम से सभी देशों को एक अन्तर्राष्ट्रीय साइबर कानून बनाना चाहिये, तो दुनिया के सभी देशों पर समान रूप से लागू हो।

संदर्भ ग्रन्थ सूची

1. पाठक, अरूण कुमार, साइबर क्राइम एवं साइबर लॉज, पुस्तक सदन प्रकाशन, इलाहाबाद 2021.
2. सिंह, डॉ0 निशान्त, साइबर अपराध, राधा पब्लिकेशन्स, नई दिल्ली, 2000.

ISSN NO.-2347-2944 (Print)
e-ISSN NO.-2582-2454 (Online)
Vol.-16, No.- I, Issues-27, YEAR- Jan.-March-2023

3. शिवराज, जैदी एम0एच0, सोशल मीडिया से साइबर अपराध, एलिया ला एजेन्सी, लखनऊ 2022.
4. India^s Cyber Security% Challenges and Options OPUS Publisher Distributors] Delhi- 2022
5. राष्ट्रीय सहारा, हस्तक्षेप साइबर हमले, 17 दिसम्बर, 2022.
6. India's Cyber Security: Challenges and Options OPUS Publisher Distributors, Delhi. 2022-
7. राष्ट्रीय सहारा, हस्तक्षेप साइबर हमले, 17 दिसम्बर, 2022.
8. https://hindi.news18.com/news/tech/indias-five-biggest-cyber-attacks-health-services-are-on-target-of-hackers-dnsh-4629473..
9. https://www.aajtak.in/technology/tech-tips-and-tricks-/story/smartphone-hack-hackers-stole-37-lakhs-from-developer-keep-these-points-in-mind-ttec-1608531-2023-01-04.
10. https://www.jagran.com/delhi/new-delhi-city-ncr-delhi-aiims-server-hack-big-disclosure-in-server-hack-case-on-sixth-day-hackers-asked-for-200-crore-cryptocurrency-23233516.html.
11. https://www.bhaskar.com/national/news/delhi-aiims-server-hacked-data-of-four-crore-patients-stolen-130604900.html.
12. https://hindi.scoopwhoop.com/artandculture/types-of-cyber-crime-fraud-cases-in-india/#amp_tf=From%20%251%24s&aoh=16 741707577640&referrer=https%3.A%2F%2Fwww.google.com&s hare=https%3A%2F%2Fhindi.sco opwhoop.com %2Fartandculture% 2Ftypes-of-cyber-crime-fraud-cases-in-india%2F.
13. https://www.amarujala.com/bizarre-news/jamtara-cyber-crime-real-story-district-of-jharkhand.
14. https://en.wikipedia.org/wiki/Crime_and_Criminal_Tracking_Network_and_Systems.
15. https://surveyofindia.gov.in/pages/national-information-security-policy-and-guidelines.
16. https://zeenews.india.com/hindi/india/steps-taken-by-the-central-government-to-spread-awareness-on-cyber-crime-prevention-1166884.
17. www.csk.gov.in/CyberSwachhtaKendra.

*****