International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

भारत में साइबर अपराध : चुनौतियाँ एवं समाधान

डॉ0 अमर सिंह[1], कु0 सपना तिवारी[2]

असिस्टेंट प्रोफेसर, समाजशास्त्र विभाग, बयालसी पी0 जी0 कालेज, जलालपुर, जौनपुर

शोधछात्रा, समाजशास्त्र विभाग, जननायक चन्द्रशेखर विश्वविद्यालय, बलिया

Email: amarsinghs1984@gmail.com

शोध सार— प्रस्तुत शोध पत्र में भारत में साइबर अपराध के विविध पक्षों पर एक विश्लेषण प्रस्तुत किया गया है। इसमें डिजिटल प्रौद्योगिकी के समाज पर बढ़ते प्रभाव से सम्बन्धित तथ्यों का विश्लेषण करने का प्रयास किया गया है। इस विश्लेषण में यह भी जानने का प्रयास किया गया है कि भारत में साइबर अपराध के कौन–कौन से तरीके हैं और वे किस प्रकार से लोगो को अपना शिकार बना रहे हैं। साथ ही साथ यह भी जानने का प्रयास किया गया है कि साइबर अपराध को नियंत्रित करने के लिए सरकार ने कौन–कौन से प्रयास किये हैं। इसमें साइबर अपराध के प्रति सर्तक रहने वाले उपायों पर भी चर्चा की गयी है।

मुख्य शब्द –स्पैम ईमेल, हैकिंग, फिशिंग, मालवेयर, विशिंग, साइबर बुलिंग, साइबर स्टॉकिंग, हैशटैग।

I. प्रस्तावना –

कम्प्यूटर और नेटवर्क आधारित अपराध को साइबर अपराध की श्रेणी में रखा जाता है। इसमें कम्प्यूटर प्रौद्योगिकी के ज्ञान का दुरूपयोग समाजविरोधी, गैर–कानूनी और अनैतिक कार्यों के लिए किया जाता है। इसमें कम्प्यूटर प्रौद्योगिकी में दक्ष व्यक्ति द्वारा कम्प्यूटर के माध्यम से विभिन्न आँकड़ों और सामग्रियों को अवैध, अनैतिक और अनाधिकृत रूप से उपयोग और प्रसारित किया जाता है। इस कारण ऐसे अपराध को इलेक्ट्रॉनिक अपराध भी कहा जाता है। साइबर अपराध के अन्तर्गत हैकिंग, रैंसमवेयर, साइबर बुलिंग, पाइरेसी, फर्जी बैंक कॉल, सोशल नेटवर्किंग साइटों पर अफवाह फैलाना, ऑनलाइन धोखाधड़ी, कम्पयूटर के माध्यम से गबन करने, गुप्त आँकड़ों की चोरी करने, अश्लीलता को प्रोत्साहन देने आदि जैसी अवैध गतिविधियाँ शामिल है। जो लोग साइबर अपराध करते है, उन्हें हैकर, स्कैमर्स या धोखेबाज कहा जाता है। **जेम्स ए0 शयूटजर** ने साइबर अपराध को परिभाषित करते हुए लिखा है, ''ऐसे सभी अपराध, जिसके लिए कम्प्यूटर अथवा उसके संगठन भागों जैसे– टर्मिनल या नेटवर्क आदि का उपयोग आवश्यक होता है, उन्हें साइबर अपराध कहा जाता है।'' **डॉन बी0 पार्कर** के शब्दों में, ''कोई भी वह अवैधानिक कार्य, जिसे पूरा करने के लिए कम्प्यूटर प्रौद्योगिकी के परिचालन का विशेष ज्ञान आवयश्यक होता है, उसे हम साइबर अपराध कहते है।'' साइबर अपराध से किसी व्यक्ति या देश की सुरक्षा और वित्तीय स्वास्थ्य को खतरा हो सकता है। सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत ऐसे कृत्यों को अपराध की श्रेणी में रखा गया है।

साइबर अपराध, अपराध का एक नया तरीका है। यह एक प्रकार की कम्प्यूटर जालसाजी है, जिसके लिए कम्प्यूटर प्रौद्योगिकी के उच्च ज्ञान की आवश्यकता होती है। इन अपराधों की प्रकृति अत्यन्त गुप्त और एकाकी होती है। इसी कारण दूसरे प्रकार के अपराधों की तुलना में साइबर अपराध को पकड़ पाना बहुत कठिन होता है। वर्तमान में साइबर अपराधों के क्षेत्र में लगातार वृद्धि होती जा रही है। इन अपराधों का सम्बन्ध आर्थिक, सैनिक, सांस्कृतिक, राजनीतिक, सामुदायिक अथवा व्यक्तिगत किसी भी पक्ष से हो सकता है। ये अपराध राष्ट्रीय जीवन से लेकर अन्तर्राष्ट्रीय उद्देश्यों तक के लिए किए जाते हैं।

II. साइबर स्पेस

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

नई तकनीकों के उन्नयन, उदारीकरण, वैश्वीकरण और मशीनीकरण के इय युग में सुलभता और सुविधाओं के नए–नए आयाम खुले हैं। आज इंटरनेट ने पूरी दुनिया को एक साथ जोड़ कर एक छोटा सा गाँव बना दिया है। इंटरनेट वैश्विक स्तर पर एक–दूसरे से जुड़े कई कम्प्यूटरों का वृहत् जाल (नेटवर्क) है, जो इंटरनेट प्रोटोकॉल के माध्यम से दुनियाभर के इलेक्ट्रॉनिक उपकरणों को एक साथ जोड़ता है। इस वृहत् नेटवर्क से जुड़कर बनने वाले वातावरण या व्यवस्था को **साइबर स्पेस** कहते है। साइबर स्पेस एक संवादात्मक डोमेन है, जो डिजिटल नेटवर्क से बना होता है। जिसके अन्तर्गत इंटरनेट के जरिये किये जाने वाले कार्य जैसे– ईमेल भेजना, चैटिंग करना, ब्राउजिंग करना, डेटा ट्रांसफर करना इत्यादि आते है। इस साइबर स्पेस से कई सारी अवधारणाएँ जुड़ी हुई है, जैसे– साइबर सिक्योरिटी, साइबर वार, साइबर क्राइम, साइबर टरेरिज्म आदि। इंटरनेट और इससे निर्मित साइबर स्पेस ने मानव सभ्यता के परिवर्तन में बड़ी क्रांतिकारी भूमिका निभाई है। इसके माध्यम से पलक झपकते ही एक टच मात्र से डेटा, सूचना एक स्थान से दूसरे स्थान पर पहुँचना, वीडियो क्रॉन्फ्रेसिंग, बिल पेमेंट तथा पैसों का ट्रांसफर हो सकता है। आज डिजिटल प्रौद्योगिकी ने 'वसुधैव कुटुम्बकम्'' की संकल्पना को व्यवहारिक बनाने में महत्वपूर्ण भूमिका निभाई है।

III. डिजिटल प्रौद्योगिकी की विभिन्न क्षेत्रों में उपयोगिता

डिजिटल प्रौद्योगिकी के द्वारा ई–गवर्नेस के माध्यम से **प्रशासनिक कार्यों**के मार्ग को भी सुलभ बनाया गया है। इनके प्रयोग से प्रशासनिक क्षेत्र में काफी सुधार आया है। डिजिटल प्रौद्योगिकी के माध्यम से कार्य में देरी, लालफीता शाही, भ्रष्टाचार आदि में बहुत हद तक कमी आई है तथा निष्पक्षता एवं पारदर्शिता बढ़ी है। अब कई तरह के प्रमाण–पत्र लेने या किसी योजना की जानकारी का लाभ लेने के लिए दफ्तरों के चक्कर काटने नही पड़ते हैं। सारी सुविधाएँ बस एक क्लिक में इंटरनेट पर उपलब्ध है।

शिक्षा के क्षेत्र में डिजिटल प्रौद्योगिकी ने तो क्रान्ति ही ला दी है। आज जटिल से जटिल अवधारणाओं के समाधान ऑडियो–वीडियो तथा हाइपरटेक्स्ट फॉर्मेट में उपलब्ध है। दुनिया भर की किताबें, लब्ध प्रतिष्ठित विद्वानों, प्रोफेसर्स के लेक्चर, अच्छे–अच्छे विश्वविद्यालयों के शोध कार्य अब आसानी से उपलब्ध है। अब तो ऑनलाइन कोर्सेज, ऑनलाइन कक्षाओं का प्रचलन भी तेजी से बढ़ रहा है। अब जिज्ञासु व्यक्ति अगर चाहे तो घर बैठे एक साथ कई चीजे सीख सकता है। डिजिटल आर्काइव्स ने पुरानी पड़ती जा रही पाण्डुलिपियों को तो जैसे नया जीवन ही दे दिया है। अब वे इंटरनेट के जरिये सुरक्षित व सर्वसुलभ भी हो पा रही है।

डिजिटल अर्थव्यवस्था एक ऐसी अर्थव्यवस्था है, जिसमें अधिकांश आर्थिक क्रियाएँ ऑनलाइन यानी इंटरनेट के माध्यम से सम्पन्न की जाती है। जिसके परिणामस्वरूप भारतीय अर्थव्यवस्था, कैशलेस अर्थव्यवस्था की ओर तीव्र गति से बढ़ रही है। कृषि, उद्योग, व्यापार, सेवा, पर्यटन, शिक्षा, बैंकिंग आदि क्षेत्रों में डेबिट कार्ड, क्रेडिट कार्ड, ई–पेमेंट, मोबाइल बैंकिंग आदि का तीव्र गति से प्रचलन बढ़ रहा है। नकदी प्रधान अर्थव्यवस्था में भ्रष्टाचार, कालाधन उग्रवाद, घूसखोरी आदि को अधिक प्रश्रय मिलता है, जबकि कैशलेस अर्थव्यवस्था में एक साथ इन सारी समस्याओं पर बहुत हद तक नियंत्रण होता है। डिजिटल अर्थव्यवस्था आतंकियों व नक्सलियों को की जाने वाली फण्डिंग को भी रोकने का कार्य करेगी, जो अन्ततः कानून व्यवस्था को बेहतर बनाने में मददगार होगी। इसके अलावा यह कल्याणकारी योजनाओं में होने वाले धन के रिसाव को भी रोकेगी, जिससे लाभार्थी को त्वरित व ईमानदारीपूर्वक पूर्ण हक प्राप्त हो सकेगा। इस प्रकार डिजिटल अर्थव्यवस्था, विकासशील अर्थव्यवस्था को विकसित अर्थव्यवस्था बनाने के मार्ग को प्रशस्त करती है।

व्यवसाय व सेवा क्षेत्र में भी डिजिटलाइजेशन के द्वारा उत्पाद के निर्माण, उसकी बिक्री तथा उसकी लागत को ज्यादा उपभोक्ता अनुकूल बनाया जा सका है। **कृषि क्षेत्र** में डिजिटलाइजेशन के द्वारा मौसम पूर्वानुमान को ज्यादा सटीक बनाकर किसानों की मदद की जा रही है। इसके माध्यम से बीज, उर्वरक, कीटनाशक आदि आगतों तक किसानों की पहुँच सरल हुई है तथा कृषि बाजार में मूल्यों को लेकर किसानों मे सजगता भी बढ़ी है। 'सुविधा एप', 'ई–नाम', 'डी डी किसान' जैसी ऑनलाइन माध्यमों के द्वारा कृषि विकास को ज्यादा तेजी से बढ़ावा मिला है।

डिजिटल प्रौद्योगिकी ने **सामाजिक व्यवस्था** में क्रांतिकारी परिवर्तन किये है। आज का समाज केवल गाँव या शहरों तक सीमित नही है, बल्कि वह इंटरनेट के माध्यम से देश–विदेश की सभ्यता और संस्कृति को समझ रहा है और उन्हें अपना भी रहा है। डिजिटल प्रौद्योगिकी ने संस्कृतियों के आदान–प्रदान में महत्वपूर्ण भूमिका अदा की है। इसने स्वास्थ्य सम्बन्धी जानकारी एवं पर्यावरण सम्बन्धी जागरूकता भी फैलाई है। सोशल मीडिया के माध्यम से ऐसी खबरें, जो कॉरपोरेट मीडिया द्वारा दब जाती थी या दबा दी जाती थी, अब लोगों के सामने आने लगी है। सोशल मीडिया ने लागों में राजनीतिक जागरूकता भी फैलाई है। लोग अब देश–विदेश की राजनीति को समझ रहे है। राजनीतिक शुचिता की मुहिम जो पहले एक स्वर नही हो पाती थी, सोशल मीडिया ने उसे सामूहिक स्वर दिया है। इसके

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

माध्यम से लोगों को अपनी भावनाओं को अभिव्यक्त करने के लिये उचित प्लेटफार्म मिला। कई ऐसी प्रतिमाएँ जो उचित संसाधनों के अभाव में दबी छुपी रह जाती थी, सोशल मीडिया ने उन्हें उभरने का मौका दिया। इस प्रकार इंटरनेट एवं साइबर स्पेस ने सामाजिक, आर्थिक और राजनीतिक स्तर पर कई ऐसे परिवर्तन किये, जिन्हें वरदान से कम नहीं माना जा सकता।

IV. भारत में साइबर अपराध

हम जितनी तेजी से डिजिटल दुनिया की ओर बढ़ रहे है, ठीक उतनी ही तेजी से साइबर अपराधों की संख्या में भी वृद्धि हो रही है और उसी के साथ हमारी निर्भरता भी इंटरनेट पर बढ़ती जा रही है। आज इंटरनेट के माध्यम से एक जगह पर बैठकर हमारी पहुँच विश्व के प्रत्येक कोने तक सम्भव हो पायी है। आज के दौर में मनुष्य हर वो चीज जिसके विषय में सोच सकता है, उस तक उसकी पहुँच इंटरनेट के माध्यम से हो सकती है, जैसे कि सोशल नेटवर्किंग, ऑनलाइन शॉपिंग, डेटा स्टोर करना, गेमिंग, ऑनलाइन स्टडी, ऑनलाइन जॉब आदि। आज के समय में इंटरनेट का उपयोग लगभग प्रत्येक क्षेत्र में किया जा रहा है। ज्यों–त्यों डिजिटल प्रौद्योगिकी हमारे निजी एवं कामकाजी जीवन तथा संचार का हिस्सा बनती जा रही है और कम्प्यूटरीकरण तथा इंटरनेट कनेक्टिवटी सरकारी कामकाजी तंत्र की अनिवार्यता बनते जा रहे हैं, त्यों–त्यों इंटरनेट के जरिये आंतरिक सुरक्षा के लिए चुनौतियाँ भी बढ़ती जा रही हैं। इंटरनेट पर उपस्थित हर सामान्य एवं महत्वपूर्ण कम्प्यूटर एक समान संचार तंत्र से जुड़ा हुआ है और यही उसकी स्थिति को संवेदनशील बना देता है। साइबर अपराधों के माध्यम से विध्वंसक गतिविधियों को अंजाम देने की प्रक्रिया ने अब सुसंगठित और संस्थागत रूप ले लिया है। साइबर अपराध आज एक गंभीर चुनौती बन गया है। साइबर टेररिज्म और साइबर वार के खतरे भी लगातार बढ़ते जा रहे है। इंटरनेट के जरिये हो रही आईएसआईएस (ISIS) की भर्तियां, मुंबई के हमलों और चीनी हैकरों की हरकतों ने स्पष्ट कर दिया है कि हमारी आन्तरिक सुरक्षा के प्रति साइबर चुनौती कितनी गम्भीर है।

आजकल विध्वंसक तत्व इंटरनेट एवं अन्य डिजिटल माध्यमों का प्रयोग कई रूपों में करने लगे है। चूँकि इंटरनेट विश्वव्यापी है, इस पर अपराधी आसानी से अपनी पहचान छुपा कर, किसी भी आपराधिक नेटवर्क के लिए आन्तरिक संदेशों का आदान–प्रदान आसानी से कर लेते है। ईमेल और चैट जैसे इंटरनेट के पारस्परिक माध्यमों के साथ–साथ आपराधिक तत्वों ने अब कई आधुनिक सेवाओं, तकनीकों और युक्तियों के जरिये संदेश भेजने शुरू कर दिये है। ऐसे लोग अपनी कोई पहचान छोड़े बिना वायस ओवर इंटरनेट प्रोटोकॉल (VOIP) के जरिये दुनिया भर में टेलीफोन कॉल करते है और ट्विटर जैसी माइक्रोब्लागिंग सेवाओं का प्रयोग कर एक–दूसरे की गतिविधियों से अवगत रहते है।

इंटरनेट पर निजता के हनन की समस्या निरन्तर गंभीर होती जा रही है। इंटरनेट ने जिस प्रकार सूचनाओं के भ्रमजाल को फैलाया है, उससे समाज में एक विकट स्थिति उत्पन्न हो गई है। आज हैकिंग, साइबर बुलिंग, फिशिंग, फार्मिंग आदि की वजह से लोग परेशान है। इनके शिकार भावुक लोग, बच्चे, किशोर एवं युवतियाँ अधिक होती है। कई बार ये समस्याएँ इतनी गंभीर हो जाती है कि लोग आत्महत्या जैसे कदम भी उठाने को मजबूर हो जाते है। वर्तमान दौर में इंटरनेट पर गलत सूचनाओं के प्रसार की एक आँधी चल पड़ी है। किसी भी खबर को अन्य भड़काऊ खबरों के साथ जोड़कर समाज में वैमनस्यता फैलाना आम हो गया है। साम्प्रदायिक दंगे फैलाने के लिये कुछ लोग गलत तरीके से वीडियों या फोटो एडिटिंग कर इसके साथ भड़काऊ संदेश प्रसारित करते है, जिससे समाज में वैमनस्य बढ़ता है। आए दिन होने वाले दंगों के पीछे इंटरनेट एवं सोशल मीडिया की बड़ी भूमिका पाई गई है। आजकल इंटरनेट का प्रयोग राजनेता भी अपने पक्ष में कृत्रिम तरीके से माहौल तैयार करने के लिए करते है। सोशल मीडिया में किसी की इमेज को बढ़ाना या निकृष्ट दिखाना अब सामान्य हो गया है। अब तो राजनीतिक दलों का प्रायः एक सोशल मीडिया विंग होती है, जो बिल्कुल प्रायोजित तरीके से किसी को गाली–गलौच करने, ट्रोल करने से लेकर किसी के पक्ष या विपक्ष में माहौल तैयार करने का काम करते है।

भारत में डिजिटल प्रौद्योगिकी के बेरोकटोक इस्तेमाल आंतरिक सुरक्ष के लिए गंभीर चुनौतियां प्रस्तुत कर रहा है। भारत में डिजिटल साक्षरता की भी कमी है, जिसकी वजह से साधारण लोग अपराधियों के चक्कर में आ जाते है एवं उन्हें कई प्रकार की समस्याओं का सामना करना पड़ता है। अनजाने कॉल कर डाटाओं की चोरी करना, एटीएम तथा अन्य मोबाइल वॉलेट से पैसे उड़ा लेना, आदि अपराध, साइबर अपराध के ही श्रेणी में आते है। इंटरनेट पर प्रकाशित सामग्री की प्रामाणिकता की जाँच की समुचित व्यवस्था नही होने के कारण भी भ्रामक सूचनाओं के प्रसार को बढ़ावा मिल रहा है।

V. साइबर अपराध के प्रकार

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

साइबर अपराध को निम्नलिखित आधारों पर बाँटा जा सकता है –

1. कम्प्यूटर से सम्बन्धित अपराध –

(i) जानकारी चोरी करना –किसी के भी कम्प्यूटर से उसकी व्यक्तिगत जानकारी निकालना– जैसे की उपयोगकर्ता के नाम या पासवर्ड।

(ii) जानकारी मिटाना –किसी के कम्प्यूटर से कोई महत्वपूर्ण जानकारी मिटाना ताकी उसे नुकसान हो।

(iii) फेर बदल करना –किसी जानकारी में कुछ हटाकर या उसमें कुछ जोड़कर, उस जानकारी को बदल देना।

(iv) बाहरी नुकसान – कम्प्यूटर के बाहरी भागों को नष्ट करना या उसे तोड़ना या भागों की चोरी करना भी कम्प्यूटर अपराध की श्रेणी में आता है।

कम्प्यूटर प्रणाली से सम्बन्धित विभिन्न प्रकार के अपराधों का क्षेत्र इतना व्यापक है कि वर्तमान युग में यह सम्पूर्ण मानवता के लिए एक बड़ा खतरा बन गया है।

2. कम्प्यूटर नेटवर्क से सम्बन्धित अपराध –

इस वर्ग के अन्तर्गत ऐसे सभी साइबर अपराध आते है, जिनका सम्बन्ध कम्प्यूटर नेटवर्क से होता है।

(i) स्पैम ईमेल –अवांछित संदेश लोगों को भेजना स्पैम कहलाता है, जिसका उद्देश्य कम्प्यूटर का डाटा चोरी करना या कम्प्यूटर को नुकसान पहुँचाना हो सकता है। ऐसे ईमेल से कम्प्यूटर में खराबी आ जाती है।

(ii) हैकिंग – किसी की भी व्यक्तिगत जानकारी को हैक करना जैसे बिना आपकी अनुमति के हैकर्स आपके कम्प्यूटर में संग्रहीत फाइलों को देखते है, एडिट करते है और नया फाइल बनाते है या आवश्यक फाइलों को मिटा देते है।

(iii) फिशिंग –इसमें जालसाज द्वारा फर्जी ईमेल भेजा जाता है और जैसे ही शिकार व्यक्ति अपने पासवर्ड या पिन की जानकारी जालसाज की वेबसाइट पर डालता है, शिकार व्यक्ति की सारी महत्वपूर्ण जानकारी हैकर के पास आ जाती है। इस प्रकार फिशिंग के माध्यम से आपकी निजी जानकारी को धोखेबाजी के माध्यम से चुरा लेते है और उसका गलत उपयोग करते है।

(iv) मालवेयर – यह सबसे अधिक पाया जाने वाला साइबर फ्राड है, जिसमें कोई भी असावधान व्यक्ति झांसे में आ कर फेक मेल एटेचमेंट को डाउनलोड कर सकता है इसे डाउनलोड करते ही मालवेयर आपके फोन, कम्प्यूटर से सारी महत्वपूर्ण जानकारियाँ निकालने में सफल हो जाता है।

(v) सिम क्लोनिंग –इसका प्रयोग वर्तमान समय में काफी बढ़ा है, जब से बैंकों ने अपने एप में या एटीएम से पैसे निकालने में ओटीपी को अनिवार्य किया है। यदि जालसाज आपके सिम को क्लोन कर लेने में सफल हो गया तो वह यूपीआई पिन को बदलने के साथ सब कुछ कर सकता है। इससे वह आपके बैंक खाते तक पहुँच बना सकता है।

(vi) विशिंग –जालसाज बैंक के प्रतिनिधि बन कर शिकार से सभी जानकारियाँ जैसे एटीएम का विवरण पिन पासवर्ड आदि शिकार से प्राप्त कर खाते से रकम उड़ा ले जाते है।

(vii) वायरस फैलाना –साइबर अपराधी कुछ ऐसे सॉफ्टवेयर आपके कम्प्यूटर पर भेजते है, जिसमें वायरस छिपे हो सकते हैं, इनमें वायरस वर्म, टार्जन हार्स, लॉजिक हार्स आदि वायरस शामिल है, यह आपके कम्प्यूटर को काफी हानि पहुँचा सकते है।

(viii) सॉफ्टवेयर पाइरेसी –नकली सॉफ्टवेयर तैयार कर सस्ते दामों पर बेचना भी साइबर क्राइम के अन्तर्गत आता है। इससे सॉफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ाता है, साथ ही साथ आपके कीमती उपकरणों को भी क्षति पहुँचती है।

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

(ix) फर्जी बैंक कॉल –आपको जाली ईमेल, मैसेज या फोन कॉल प्राप्त हो जो आपके बैंक जैसा लगे, जिसमें आपसे पूछा जाये कि आपके एटीएम नम्बर और पासवर्ड की आवश्यकता है और यदि आपके द्वारा यह जानकारी नहीं दी गयी तो आपका खाता बन्द कर दिया जायगा या इस लिंक पर सूचना दें। जबकि वास्तविकता यह है कि बैंक कभी भी इस प्रकार की जानाकरी को ईमेल, मैसेज या फोन कॉल से नही मांगता।

(x) सोशल नेटवर्किंग साइटों पर अफवाह फैलाना –बहुत से लोग सोशल नेटवर्किंग साइटों पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते है, लेकिन यूजर्स उनके इस इरादे को समझ नहीं पाते है और जाने–अनजाने में ऐसे लिंक्स को शेयर करते रहते है, लेकिन यह कृत्य भी साइबर अपराध की श्रेणी में आता है।

(xi) साइबर बुलिंग –

किसी व्यक्ति को सूचना प्रौद्योगिकी से जुड़े माध्यमों के जरिये बार–बार और जानबूझकर अशोभनीय कमेंट करना, अपमानित करना, धमकिया देना, मजाक बनाने जैसी गतिविधि करने को साइबर बुलिंग कहते हैं। इसकार्य के लिए सोशल नेटवर्किंग वेबसाइट्स, ब्लॉग्स, ईमेल आदि का प्रयोग किया जाता है। अधिकांश बच्चे और किशोर साइबर बुलिंग का शिकार होते है। इससे इनके सेहत पर भी असर पड़ता है और कभी–कभी तो आत्महत्या भी कर लेते है। माइक्रोसॉफ्ट की ओर से कराए गए एक सर्वेक्षण से पता चलता है कि भारत के 53 प्रतिशत बच्चे इस समस्या से परेशान है।

(xii) साइबर स्टॉकिंग –

साइबर स्टॉकिंग योजनाबद्ध तरीके से किसी पर नजर रखने, उसके निकट जाने की कोशिश करने और अपनी हरकतों से उसके मन में आशंका या भय पैदा कर देने से सम्बन्धित है। इस प्रक्रिया में निजता का घोर हनन होता है, जो एक संज्ञेय अपराध है। साइबर स्टॉकिंग की सर्वाधिक शिकार महिलाएँ होती है। सोशल नेटवर्किंग माध्यमों, ईमेल, चैट–रूम्स, मैसेजिंग आदि ने साइबर स्टॉकिंग न केवल बढ़ावा दिया है, बल्कि किसी का चौबीस घण्टे पीछा करना भी सम्भव बना दिया है।

(xiii) हैशटैग –

सोशल नेटवर्किंग माध्यमों पर साइबर अपराधियों द्वारा हैशटैग का भी जमकर दुरुपयोग किया जाने लगा है, जो किसी भी व्यक्ति के नाम से हैशटैग बनाकर ऊल–जलूल टिप्पणियाँ डालने लगते है। हैशटैग युक्त टिप्पणियाँ अधिक आसानी से दूसरों की नजरों में आ जाती है और वे भी प्रतिक्रिया करते हुए चर्चा के लिए आ जुटते है। इंटरनेट और दूर संचार साधनों की मुक्त प्रकृति पूरी दुनिया के लिए बहुत महत्वपूर्ण है, लेकिन साइबर अपराधियों ने इसे एक समस्या बना दिया है।

(xiv) गबन और जालसाजी –

सलामी तकनीक, साइबर अपराध से जुड़ी हुई गबन और जालसाजी की एक विशेष तकनीक है, जिसके द्वारा किसी व्यापारिक प्रतिष्ठान, कम्पनी या बेंक में जमा हजारों–लाखों ग्राहकों की धनराशि के कुछ अंश को बहुत परिष्कृत ढंग से चुरा लिया जाता है। इसके बाद भी बैंक या कम्पनी में राशि के लेन–देन का योग उतना ही रहता है। जमाकर्ताओं की छोटी–छोटी राशियों की चोरी से अपराध करने वाले व्यक्तियों को बहुत अधिक धन प्राप्त हो जाता है।

(xv) अश्लीलता एवं अभद्रता सम्बन्धी अपराध –

सूचना प्रौद्योगिकी के माध्यमों से अश्लीलता और अभद्रता को बहुत अधिक प्रोत्साहन भी मिलता है। आज विभिन्न क्षेत्रों में ऐसें साइबर अपराधों में तेजी से वृद्धि हो रही है, जिसका उद्देश्य नई पीढ़ी को गुमराह करके वैयक्तिक विघटन में वृद्धि करना होता है। आज कम्प्यूटर से सम्बन्धित अनेक ऐसी तकनीकें विकसित हुई है, जिसकी सहायता से किसी विशेष व्यक्ति की भाव–भंगिमा अथवा चित्र को किसी भी तरह चित्रित करके प्रस्तुत किया जा सके। इससे पोर्नोग्राफी और ब्लैकमेलिंग जैसे अपराधों में भी वृद्धि हुई है।

VI. भारत में साइबर अपराधों के विरूद्ध कानूनी प्रयत्न

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

(I) सूचना प्रौद्योगिकी अधिनियम – 2000

30 जनवरी 1997 को संयुक्त राष्ट्र की जनरल एसेंबली में पारित प्रस्ताव संख्या 51/162 के आधार पर भारत में सूचना प्रौद्योगिकी अधिनियम 9 जून सन् 2000 को लागू हुआ। इसे साइबर अपराध कानून भी कहा जाता है। यह कम्प्यूटर सिस्टम, कम्प्यूटर नेटवर्क और इलेक्ट्रानिक उपकरण में डेटा एंव सूचना को नियंत्रित करता है। सूचना प्रौद्योगिकी संशोधन अधिनियम 2008 के माध्यम से इसमें काफी संशोधन किया गया। इसमें निम्नलिखित प्रावधानों का उल्लेख है –

1. धारा 65 – कम्प्यूटर संसाधनों से छेड़छाड़ की कोशिश।

2. धारा 66 – कम्प्यूटर संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश।

3. धारा 66 ए – संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दण्ड का प्रावधान।

4. धारा 66 बी – कम्प्यूटर या अन्य किसी इलेक्ट्रानिक गैजैट से चोरी की गई सूचनाओं को गलत तरीके से हासिल करने के लिए दण्ड का प्रावधान।

5. धारा 66 सी – किसी की पहचान चोरी करने के लिए दण्ड का प्रावधान।

6. धारा 66 डी – अपनी पहचान छुपाकर कम्प्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुंच बनाने के लिए दण्ड का प्रावधान।

7. धारा 66 ई – किसी की निजता भंग करने के लिए दण्ड का प्रावधान।

8. धारा 66 एफ – साइबर आतंकवाद के लिए दण्ड का प्रावधान।

9. धारा 67 – आपत्तिजन सूचनाओं के प्रकाशन से जुड़े प्रावधान।

10. धारा 67 ए – इलेक्ट्रॉनिक माध्यमों से सेक्स या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दण्ड का प्रावधान।

11. धारा 67 बी – इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो।

12. धारा 67 सी – मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दण्ड का प्रावधान।

13. धारा 70 – सुरक्षित कम्प्यूटर तक अनाधिकार पहुँच बनाने से सम्बन्धित प्रावधान।

14. धारा 71 – डाटा या आंकड़ों को गलत तरीके से पेश करना।

15. धारा 72 – आपसी विश्वास और निजता को भंग करने से सम्बन्धित प्रावधान।

16. धारा 72 ए – कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से सम्बन्धित प्रावधान।

17. धारा 73 – फर्जी डिजिटल हस्ताक्षर का प्रकाशन।

18. धारा 78 – इसमें इंस्पेक्टर स्तर के पुलिस अधिकारी को इन मामलों में जांच का अधिकार हासिल है।

(II) साइबर अपराधों से निपटने की दिशा में सरकार के अन्य प्रयास –

(1) राष्ट्रीय साइबर सुरक्षा नीति–2013जारी की गई, जिसके तहत सरकार ने अति–संवेदनशील सूचनाओं के संरक्षण के लिए "राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केन्द्र" (NCIIPC) का गठन किया।

(2) सूचना सुरक्षा शिक्षा और जागरूकता परियोजना (ISEA)सूचना, सुरक्षा के क्षेत्र में अनुसंधान, शिक्षा और प्रशिक्षण प्रदान करने तथा जागरूकता बढ़ाने हेतु इस परियोजना को प्रारंभ किया गया।

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

(3) कम्प्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT-IN)की स्थापना की गयी है, जो कम्प्यूटर सुरक्षा के लिये राष्ट्रीय स्तर की मॉडल एजेंसी है।

(4) साइबर स्वच्छता केन्द्र – देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए इसकी स्थापना की गयी।

(5) भारतीय साइबर अपराध समन्वय केन्द्र – 14 सी –इसकी स्थापना जनवरी 2020 में अन्तर–एजेंसी समन्वय के लिये की गयी। जिसका उद्देश्य साइबर अपराध सम्बन्धी मुद्दों को व्यापक और समन्वित तरीके से नियंत्रित करना है।

(6) साइबर सुरक्षित भारत पहल – 2018 – इसका उद्देश्य साइबर अपराधों के प्रति लोगों में जागरूकता फैलाना है।

(7) राष्ट्रीय साइबर सुरक्षा समन्वय केन्द्र – इसकी स्थापना 2017 में की गयी। जिसका उद्देश्य वास्तविक समय में साइबर खतरों का पता लगाने के लिए देश में आने वाले इंटरनेट टरैफिक और संचार मेटाडेटा का स्कैन करना है।

(8) ऑनलाइन साइबर क्राइम रिर्पोटिंग पोर्टल– इस पोर्टल की स्थापना बाल अश्लीलता या बाल यौन उत्पीड़न या अन्य यौन सामग्री से सम्बन्धित शिकायतों की रिर्पोटिंग को सार्थक बनाने के लिए की गयी है।

(9) भारतीय कम्प्यूटर आपातकालीन प्रतिक्रिया टीम (सर्ट–इन) – इसका प्रमुख कार्य साइबर घटनाओं पर सूचना का संग्रह विश्लेषण तथा प्रसार है।

VII. साइबर अपराध को रोकने के उपाय

साइबर अपराध को नियंत्रित करने के लिए निम्नलिखित उपाय करने चाहिये –

1. साइबर अपराध को रोकने के लिए कम्प्यूटर प्रौद्योगिकी में दक्ष टीम को संगठित करना आवश्यक है। ताकि किसी भी अपराध को घटित होते ही, तुरन्त उचित कार्यवाही की जा सके।

2. इलेक्ट्रॉनिक तकनीक पर आधारित गबन और जालसाजी जैसे अपराधों को तभी कम किया जा सकता है, जब विभिन्न लेखा परीक्षकों को कम्प्यूटर का उच्च स्तरीय ज्ञान हो।

3. **भारत संचार निगम**, संचार से जुड़ी हुई एक प्रमुख संस्था है। इसे सरकार द्वारा स्पष्ट निर्देश देना चाहिए कि इलेक्ट्रॉनिक उपकरणों द्वारा किसी भी तरह की अश्लीलता या अभद्रता से सम्बन्धित कार्यक्रम प्रस्तुत न किए जा सकें।

4. व्यापक राष्ट्रीय साइबर सुरक्षा नीतियों और रणनीतियों को विकसित करने तथा लागू करने की आवश्यकता है, जो साइबर क्षेत्र में रक्षा एवं अपराध दोनों का समाधान कर सकेगी।

5. सरकारी एजेंसियों के लिए घुसपैठ पहचान हेतु उन्नत प्रणाली, सुरक्षित नेटवर्क और साइबर सुरक्षा प्रशिक्षण के साथ–साथ साइबर बुनियादी ढाँचे को मजबूत करने हेतु संसाधन आवंटित करने की आवश्यकता है।

6. साइबर खतरों की खुफिया जानकारी साझा करने और राज्य–प्रायोजित खतरों पर प्रतिक्रियाओं का समन्वय करने के लिये अन्य देशों तथा अंतराष्ट्रीय संगठनों के साथ सहयोग करना चाहिये।

7. साइबर अपराध के लिए कठोर दण्ड की व्यवस्था करनी चाहिए।

8. महत्वपूर्ण दस्तावेजों और आंकड़ों की चोरी को रोकने के लिए पासवर्ड जटिल प्रकृति के हो तथा उनकी जानकारी केवल इनका उपयोग करने वाले व्यक्ति अथवा संस्था को ही हो।

9. इलेक्ट्रॉनिक तकनिक से सम्बन्धित महत्वपूर्ण सेवाओं में केवल उन्ही व्यक्तियों को नियुक्त करना आवश्यक है, जो संस्था एवं देश के प्रति पूरी तरह से निष्ठावान और ईमानदार हो।

10. अंजान नम्बरों से काल, मैसेज एवं ईमेल से सतर्क रहना चाहिये।

International Journal of Science and Social Science Research
ISSN: 2583-7877 Peer Reviewed & Refereed Journal
Page No: 219-226 DOI: https://doi.org/10.63671/ijsssr.v3i4.487 Volume: 3 | Issue: 4

11. पैसा प्राप्त करने के लिए किसी पिन की आवश्यकता नहीं होती। अतः यूपीआई पर Request Money में सतर्क रहें व पिन डालने से बचें।

12. फर्जी मोबाइल एप से बचें। जालसाज गूगल प्ले स्टोर पर बैंकों के फर्जी एप डाल रहे है। अतः मूल व प्रामाणिक एप का ही प्रयोग करें।

13. कभी अपना पिन किसी से साझा न करें। यूपीआई एप को biometric recognition से सुरक्षित करें, जिसे हैक नही किया जा सकता। फोन एवं कम्प्यूटर में Antivirus डाल कर रखें।

14. कोई भी अंजान सॉफ्टवेयर या प्रोग्राम डाउनलोड न करें। किसी अंजान मेल को न खोलें। हमेशा अपने ईमेल को वाइरस/मालवेयर से स्कैन करते रहे।

15. कभी भी किसी open wifi का प्रयोग न करें, जब तक कि यह विश्वसनीय न हो।

16. अपने बैंक के संदेशों व खाते की जांच करते रहना चाहिये। बैंक कभी भी एटीएम, यूपीआई पिन, ओटीपी की जानकारी नही माँगता।

VIII. निष्कर्ष

निस्संदेह डिजिटल प्रौद्योगिकी मानव सभ्यता के इतिहासकी एक बड़ी उपलब्धि है। डिजिटल प्रौद्योगिकी ने जहाँ एक ओर जीवन के प्रत्येक क्षेत्र में ढेर सारे सकारात्मक परिवर्तन किये है, तो वहीं दूसरी ओर इसके नकारात्मक प्रभाव भी कम नही है। हमे डिजिटल प्रौद्योगिकी के प्रयोग को रचनात्मक निर्माणकारी गतिविधियों की ओर मोड़ना होगा, इसके लिए आवश्यक है कि डिजिटल प्रौद्योगिकी के माध्यमों पर **'सूचना के विस्फोट'** का सही ढंग से नियमन किया जाये, लोगों को डिजिटल साक्षरता के प्रति जागरूक किया जाय तथा इसके साकारात्मक पक्षों को सबल बना कर, इससे उत्पन्न होने वाले नकारात्मक प्रभावों पर विजय प्राप्त की जाये। अब इंटरनेट क्रान्ति अपने पाँचवी पीढ़ी में पहुँच चुकी है, ऐसे में जरूरी है कि हम समय रहते डिजिटल प्रौद्योगिकी आधारित समस्याओं के समाधान को ढूंढ लें। आने वाला समय इंटरनेट ऑफ थिंग्स (IOT) का है, जिसमें कार्य बिग डेटा एनालिसिस पर आधारित ऑटोमेशन द्वारा निष्पादित होंगे। बहुत ही जल्द हम इंटरनेट पर इतने आश्रित हो जायेंगे कि वह एक पर्सनल असिस्टेंट की भाँति हमारे सभी कार्य स्वतः करने में सक्षम होगा। आने वाले दिनों में जब हम एक डिजिटल प्रौद्योगिकी क्रान्ति के युग में प्रवेश करने जा रहे है, ऐसे में यदि हमने डिजिटल प्रौद्योगिकी को सुरक्षित एवं भरोसेमंद बनाने में सफलता प्राप्त कर ली तो यह अवश्य ही एक वरदान साबित होगा, अन्यथा जिस गति से साइबर अपराधों की संख्या में वृद्धि हो रही है, ऐसे में इसे अभिशाप बनते भी देर न लगेगी।

संदर्भ ग्रंथ –

1. अग्रवाल, डॉ0 गोपाल कृष्ण, भारत में सामाजिक समस्याएं एवं विकास के मुद्दे, आगरा, एस. बी. पी. डी. पब्लिशिंग हाउस, 2023

2. Morre, Robert, Cybercrime: Investigating High-Technology Computer Crime, UK, Routledge Publishing, 2015

3. Chandan, Harish, Cyber Laws and IT Protection, New Delhi, PHI Learning Private Limited, 2012

4. Halber, Debarati & K. Jaishankar, Cyber Crime andThe Victimization of Women : Laws, Right and Regulations, USA, IGI Global, 2011

5. Jain, Rohit Arvind, Cyber Crime & Law, Chattisgarh, Evincepub Publishing, 2018

6. कुरुक्षेत्र, नई दिल्ली, प्रकाशन विभाग, दिसम्बर 2022