ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 8.4
IJAR 2021; SP7: 105-108

रविकांत
(असिस्टेंट प्रोफेसर) नॉर्थ इंडिया कॉलेज ऑफ लॉ, नजीबाबाद (बिजनौर), उत्तर प्रदेश, भारत

Editors

Dr. Parmil Kumar
(Associate Professor),
Sahu Jain (P.G) College, Najibabad (Bijnor), Uttar Pradesh, India

Faiyazurrehman
(Research Scholar),
Dr. Bhimrao Ambedkar University, Agra), Uttar Pradesh, India

Dr. Anurag
(Principal),
Baluni Public School Tallamotadak, Najibabad), Uttar Pradesh, India

Corresponding Author:
रविकांत
असिस्टेंट प्रोफेसर, नॉर्थ इंडिया कॉलेज ऑफ लॉ, नजीबाबाद, बिजनौर, उत्तर प्रदेश, भारत

(*Special Issue*)
"Twenty-First Century: Cultural and Economic Globalization"

साइबर अपराधीकरण के संदर्भ में सोशल मीडिया का प्रभाव (2020–2021)

रविकांत

DOI: https://doi.org/10.22271/allresearch.2021.v7.i7Sc.8688

सारांश

साइबर अपराध से जुड़ा यह शोध–पत्र वैश्विक दृष्टि से 2020 व 2021 से जुड़ी साइबर अपराध की घटनाओं का उल्लेख करता है विशेषकर कोविड–19 महामारी के दौरान साइबर संसार के अंग कंप्यूटर और कंप्यूटर नेटवर्क के माध्यम से सोशल मीडिया प्लेटफॉर्म पर हो रहे अपराध जैसे लोगों की निजता का हनन व अन्य अपराधों को दर्शाता है। सोशल मीडिया तथा अन्य प्रकार के साइबर अपराधों व इससे होने वाली हानियों के विषय में विभिन्न साइट्स के माध्यम से आंकड़े जुटाकर प्रस्तुत करने का प्रयास किया गया है। साइबर संसार के विकास में डिजिटल क्रांति की महत्वपूर्ण भूमिका के कारण इस संसार में अनेक सामाजिक बदलाव देखने को मिले हैं जिस कारण लोगों की परंपराओं व संस्कृति में बदलाव आया हैं। डिजिटल क्रांति के युग में साइबर संसार से जुड़ी महत्वपूर्ण जानकारियों का होना भी अति आवश्यक है इसलिए इस शोध–पत्र के माध्यम से जागरूकता एवं निजता के विषय को भी उजागर किया गया है।

कूटशब्दः साइबर संसार, सोशल मीडिया, कोविड–19, साइबर अपराध, निजता

प्रस्तावनाः

21 वी शताब्दी के प्रवेश में मानव को अनेकों सुविधाएं प्राप्त हुई, जिसमें आर्थिक विकास, रोजगार के बढ़ते साधन, औद्योगिक विकास आदि महत्वपूर्ण हैं, इसका मुख्य आधार सूचना एवं प्रौद्योगिकी का विकास है जो कंप्यूटर जनित अंतरजाल (जो साइबर संसार का एक अंग है) पर आधारित है। किंतु इन लाभों के साथ–साथ मानव को अनेकों हानियों एवं समस्याओं का सामना भी करना पड़ रहा है। इन हानियों एवं समस्याओं में सबसे जटिल एवं उभरती हुई वैश्विक समस्या के रूप में साइबर अपराध में हो रही वृद्धि है। साइबर संसार की आभासी दुनिया ने वास्तविक दुनिया में अनेक परिवर्तन किये हैं। 21 वी शताब्दी में इस आभासी दुनिया का विकास इस गति से हुआ कि वर्तमान में मानव का इस इलेक्ट्रॉनिकमयी दुनिया के बिना रह पाना कठिन है। सामान्य तौर पर 'साइबर संसार' एक ऐसा 'आभासी संसार' है जो प्रकाश तंतु और संकेतों आदि या इसके सूक्ष्म कणों से भरा है इसमें अनेक गतिविधियां देखने योग्य नहीं है तथा अनेक गतिविधियां देखने योग्य तो हैं किंतु उसे छू नहीं सकते इसलिए इसे आभासी संसार कहा जाता है अर्थात यह इलेक्ट्रॉनिक माध्यम के संगणक (computer) एवं अंतरजाल प्रणाली (network system) पर आधारित है जिसमें आंकड़ों का संग्रहण, संशोधन, आदान–प्रदान एवं सजीव संवाद होता है। साइबर संसार या आभासी दुनिया में मानव उत्थान की अनेक क्षमताएं एवं संभावनाएं हैं और इसका श्रेय साइबर संसार के अंग 'सोशल मीडिया' को भी जाता है जिससे मानव जीवन शैली को नया आयाम मिला है। साइबर संसार से जुड़ी सुविधाएं इतनी सस्ती, सुलभ और रोजगार के अवसर से भरपूर होने के कारण इसका तेजी से विकास हुआ है तथा सोशल मीडिया ने इसे और आसान बना दिया है।

किंतु इतनी अपार संभावनाओं के चलते इसके विकास की राह आसान नहीं है। जहां एक ओर साइबर संसार ने विश्व को विकास का एक मंच दिया हैं, वहीं साइबर अपराधों के चलते वैश्विक स्तर पर लगातार व्यक्तियों तथा लगभग विश्व के सभी देशों को आर्थिक, सामाजिक तथा राजनीतिक

हानि का सामना करना पड़ता है। 'साइबर अपराध' ऐसे अपराध है जो संगणक तथा अंतरजाल के माध्यम से किए गए कृत्य हैं जो साइबर विधि या अन्य विधि के अनुसार वर्जित किए गए। साइबर अपराधों में 'सोशल मीडिया' के माध्यम से हो रहे साइबर हमलों की समस्या के कारण मानव की निजता का हनन, उद्योगों को आर्थिक हानि तथा अन्य प्रकार की समस्याएं उत्पन्न हुई है, इतना ही नहीं 21वीं शताब्दी में जब पूरा विश्व कोविड–19 महामारी से जूझ रहा है तो सोशल मीडिया तथा साइबर संसार के हमलों की घटनाओं में भी काफी वृद्धि हुई है। वर्ष 2021 में ही साइबर अपराध की महत्वपूर्ण घटनाओं में जैसे अमेरिका के अनेकों विश्वविद्यालय के विद्यार्थियों का निजी डेटा चोरी होना, रोजगार के लिए लाखों आवेदकों द्वारा दी गई सूचनाओं की चोरी, भारतीय फेसबुक यूजर्स के डाटा की चोरी, क्लबहाउस के डाटा की चोरी आदि जिसके कारण लोगों की निजता पर खतरा बना हुआ है।

अध्ययन का उद्देश्य

इस शोध–पत्र का मुख्य उद्देश्य सोशल मीडिया के माध्यम से हो रहे साइबर अपराधों के मामलों की जानकारी देना व सतर्कता को बढ़ावा देना है जिसके अन्य उद्देश्य निम्नलिखित हैं–

- साइबर अपराध के बारे में जागरूकता
- साइबर नियमो के पालन मे समझ
- साइबर अपराध के विरूद्ध सतर्कता
- सोशल मीडिया के परिदृश्य से साइबर अपराध
- सोशल मीडिया के माध्यम से साइबर अपराधों में हो रही वृद्धि की जानकारी देना
- कोरोना महामारी के दौर में साइबर अपराध

अनुसंधान की क्रियाविधि

यह अध्ययन आलोचनात्मक, मूल्यांकनात्मक, वर्णनात्मक, विश्लेषणात्मक और व्याख्यात्मक विधियों का उपयोग करते हुए तथा द्वितीयक स्रोतों के माध्यम से 2020–2021 में सोशल मीडिया के माध्यम से साइबर अपराध पर केंद्रित है। द्वितीयक स्रोत वह स्रोत है जो पुरानी या गैर–मूल जानकारी प्रदान करता है। द्वितीयक स्रोतों में शोध पत्र, और शोध निबंध, शोधगंगा, , ई–संसाधन, विकिपीडिया, ब्रिटानिका ,अन्य वेबसाइटें, समाचार पत्र तथा पुस्तकें भी शामिल हैं।

अध्ययन का विश्लेषण

जहां एक ओर कंप्यूटर एवं संजालीकरण के कारण डिजिटल क्रांति को बढ़ावा मिला और साइबर संसार की रचना के साथ विश्वभर में तकनीकी, प्रौद्योगिकी, रोजगार, शिक्षा , चिकित्सा आदि के क्षेत्रों में भी विकास हुआ। इसमें कोई संदेह नहीं कि कंप्यूटरीकरण एवं संजालीकरण के दौर में हम एक ओर पारदर्शिता एवं निजता का दावा करते हैं किंतु वहीं दूसरी ओर साइबर अपराधों में भी अत्यधिक वृद्धि हो रही है आज हम सोशल मीडिया साइट्स पर विश्व के लोगों के साथ एक साथ जुड़ रहे हैं किंतु साइबर अपराधी सोशल मीडिया प्लेटफॉर्म पर डाली गई हमारी निजी जानकारी को चोरी कर रहे हैं और हद तो यहां तक है कि इसके बदले यें लोग डाटा विक्रय एवं फिरौती का कारोबार कर रहे हैं जिसके कारण वैश्विक जगत में लोगों के अतिरिक्त औद्योगिक संस्थानों को भी आर्थिक हानि का सामना करना पड़ रहा है। वास्तविक दुनिया की भांति ही साइबर संसार में भी मानव कुछ महत्वपूर्ण अधिकार प्रदान किए गए हैं जिसमें सबसे महत्वपूर्ण अधिकार निजता का अधिकार है जो मानव अधिकारों के प्राण एवं दैहिक स्वतंत्रता के अधिकार का अंग है। भारतीय परिदृश्य में 'भारत का संविधान' के अनुच्छेद 21 में यह अंतर्निहित है किंतु इस अधिकार का लगातार साइबर दुनिया में हनन हो रहा हैं। वैश्विक पटल पर सोशल मीडिया प्लेटफॉर्म के अधीन उपयोगकर्ताओं के डाटा की जानकारी की चोरी हो रही है और कोविड–19 के समय में तो यह स्थिति और गंभीर हुई है जहां डाटा की चोरी बड़े पैमाने पर हो रही हैं। जहां तक साइबर संसार और निजता का प्रश्न है तो साइबर संसार में लोगों द्वारा किए जा रहे क्रियाकलाप से लोगों को यह विश्वास हो सकता है कि उनके यह कृत्य या कार्य निजता की सीमाओं के अंदर आते हैं परंतु वास्तविकता यह है कि निजता जैसी कोई चीज साइबर संसार में मायने नहीं रखती है यह मात्र कल्पना हो सकती है क्योंकि साइबर संसार में जो कुछ भी कार्य हो रहा है वह अभिलिखित (recorded) होता है जिस कारण इसे आवश्यकता के अनुसार पुनः प्राप्त किया जा सकता है और जैसे ही इसको प्राप्त करके सार्वजनिक किया जाता है वैसे ही निजता का हनन होना लाजमी है अर्थात साइबर संसार एक ऐसा संसार है जिसमें कोई भी व्यक्ति जो कोई भी कृत्य करता है वह इसमें पुनः प्राप्त किया जा सकता है चाहे वह जानकारी मिटा भी दे। हम यह समझते हैं कि वह जानकारी हमने मिटा दी तो उसका प्रयोग नहीं हो सकता किंतु साइबर संसार में ऐसा नहीं है मिटाई हुई जानकारी को भी पुनः प्राप्त किया जा सकता है और उसका दुरुपयोग हो सकता है।

कोविड–19 के दौरान साइबर अपराध की महत्वपूर्ण घटनाएं जैसे –

- अमेरिका के स्टैनफोर्ड विश्वविद्यालय के तहत आने वाली चिकित्सा संस्थान का डाटा लीक होना,
- मई 2021 में मैरिलैंड विश्वविद्यालय के विद्यार्थियों का डाटा लीक,
- कोलाराडो और मियामी विश्वविद्यालय के निजी, स्वास्थ्य व शोध से सम्बन्धित फाइल की चोरी
- वाशिंगटन राज्य आडिटर ऑफिस के अनुसार 15 लाख बेरोजगारों के आवेदनों में सूचनाओं की चोरी हुई इसके लिए उनसे वसूली भी की गई,
- अप्रैल 2021, विश्व के 100 से अधिक देशों में 53.30 करोड़ फेसबुक उपयोगकर्ताओं का निजी डाटा लीक हुआ जो लगभग 2 वर्ष पुराना डाटा था जिसमें नाम, लोकेशन, इ–मेल, मोबाइल नं. जैसी सूचनाएं थी *इस प्रकार के डाटा के लिए हैकर्स 20 डॉलर तक लेते हैं कुल मिलाकर यह 1060 करोड रुपए मूल्य का डाटा है,*
- भारतीय परिदृश्य से 60 लाख भारतीय फेसबुक यूजर्स का डाटा और फोन नंबर लीक हुए हैं
- अप्रैल 2021 में ही प्रोफेशनल नेटवर्किंग प्लेटफॉर्म लिंकडइन में भी सेंधमारी कर 50 करोड़ से ज्यादा लोगों की निजी जानकारियां चुरा लेने का खुलासा हुआ हालांकि लिंक्डइन ने इसे अपने प्लेटफार्म का मानने से इनकार कर दिया था,
- चेकप्वाइंट रिसर्च द्वारा मोबाइल सुरक्षा 2021 रिपोर्ट पेश की गई इस रिपोर्ट के अनुसार *महामारी की वजह से अक्टूबर 2020 से मार्च 2021 के दौरान देश की कारपोरेट दुनिया और विद्यार्थियों ने अपने काम और पढ़ाई के लिए बड़ी संख्या में ऑनलाइन विकल्पों को अपनाया है ऐसे में साइबर अपराधियों को वे आसान शिकार नजर आते हैं।*

वैश्विक फार्म चेक प्वाइंट सॉफ्टवेयर टेक्नोलॉजी के अनुसार 97 प्रतिशत कंपनियां व संस्थान साइबर हमलों के निशाने पर है इस रिसर्च में 46 प्रतिशत कंपनियां या संस्थान किसी ने किसी कर्मचारी या विद्यार्थी के माध्यम से सॉफ्टवेयर या ऐप डाउनलोड करने के द्वारा किसी ना किसी तरह साइबर अपराध के शिकार बनने में मदद करते हैं।

हाल ही में मई 2021 में कोविड–19 महामारी के चलते अमेरिका जैसे विकसित राष्ट्र में विश्व का सबसे प्रमुख साइबर हमला जिसमें इंधन पाइपलाइन 'कॉलोनियल पाइप लाइन' पर किया गया इसके द्वारा अमेरिकी ईस्ट कोस्ट राज्यों में डीजल, गैस और जेट ईंधन पर संकट पैदा हो गया। इस पाइपलाइन से प्रतिदिन 25 लाख बैरल तेल जाता था *हालांकि इसकी पुष्टि हो गई है कि यह हमला डार्कसाइड नाम के एक साइबर अपराधी गिरोह ने किया था।*

इसके अतिरिक्त भारत में भी चीन के हैकर्स ने कोविड–19 के दौरान भारतीय वैक्सीन निर्माता कंपनी 'सीरम इंस्टीट्यूट ऑफ इंडिया' और 'भारत बायोटेक' पर साइबर हमले की कोशिश की थी।

अक्टूबर 2020 में मुंबई के एक बड़े हिस्से की पावर ग्रिड फेल हो जाने से अंधेरा छा गया था *अमेरिका की मैसाचुसेट्स स्थित 'साइबर सिक्योरिटी कंपनी' 'रिकॉर्डेड फ्यूचर' ने अपनी एक रिपोर्ट में कहा था कि चीनी सरकार समर्थित हैकरों के एक ग्रुप में मैलवेयर के जरिए मुंबई के पावर ग्रिड को निशाना बनाया था हालांकि केंद्र सरकार ने इसे साइबर हमला नहीं माना था।*
आईबीएम की एक रिपोर्ट के अनुसार वर्ष 2020 साइबर हमलों में भारत का एशिया–प्रशांत में दूसरा स्थान था। विश्व एक तरफ कोरोना महामारी से लड़ रहा था तो दूसरी ओर जापान के बाद साइबर हमले झेलने वाला भारत का दूसरा स्थान था इन हमलों में सबसे ज्यादा साइबर हमले बैंकिंग और बीमा क्षेत्र से जुड़ी कंपनियों पर हुए।

भारत सरकार द्वारा संसद में प्रस्तुत आकड़ों के अनुसार वर्ष 2020 में लगभग 1.16 मिलियन साइबर हमले के मामले सामने आए हैं जो 2019 के आंकड़ों के लगभग 3 गुना है और 2016 के आंकड़ों से लगभग 20 गुना है औसतन लगभग 3000 साइबर हमलों के मामले वर्ष में प्रतिदिन होते हैं।

'कंप्यूटर इमरजेंसी रिस्पांस टीम' जो साइबर हमलों से बचाने का भारतीय संस्थान हैं की एक रिपोर्ट के अनुसार वर्ष 2019 में साइबर हमलों के मामले 394499 थे जो 2020 में बढ़कर 1158208 मामलें हो गये। भारत में 2017 के अनुसार 53117 साइबर हमले के मामले थे, 2018 में 208456 मामले, 2019 में 394499 तथा 2020 में 1158208 मामलें हैं रिसर्च फर्म और विशेषज्ञों के अनुसार वर्ष 2021 में लगभग सभी क्षेत्रों जैसे निर्माण, सेवा, शिक्षा, स्वास्थ्य आदि क्षेत्रों में और अधिक साइबर हमलों की संभावना है।

साइबर हमलों से सुरक्षा के लिए पहली अंतरराष्ट्रीय संधि 'बुडापेस्ट सम्मेलन' के दौरान हुई जो साइबर अपराध को रोकने के लिए घरेलू विधियों में तालमेल बैठाने, अन्वेषण तकनीकी को बढ़ावा देने और राष्ट्रों के बीच समन्वय को बढ़ावा देने के लिए हुई। इस संधि का मुख्य उद्देश्य संजालों और अन्य कंप्यूटर संजालों के साथ हो रहे अपराधों जिनमें विशेषकर कॉपीराइट का उल्लंघन, कंप्यूटर जनित कपट, बाल–वेश्यावृत्ति , घृणित अपराध और संजाल सुरक्षा का उल्लंघन शामिल है इसकी मुख्य विशेषताएं इसकी उद्देशिका में समाहित है जिसमें साइबर अपराध के विरुद्ध समाज की रक्षा शामिल है जिसके अन्तर्गत उपयुक्त विधायक और अंतरराष्ट्रीय सहभागिता को बढ़ावा देना इसकी उदेशिका का मूल है अन्य विशेषताओं में

- घरेलू अपराधिक विधियों के अपराध तत्वों को साइबर अपराध से जोड़ना,
- अन्वेषण व विचारण के लिए आवश्यक घरेलू प्रक्रियात्मक विधियों की उपलब्धता आदि इसके अन्य उद्देश्य हैं

निष्कर्ष

भारतीय परिदृश्य के अनुसार साइबर अपराध के विरूद्ध भारत में सूचना प्रौद्योगिकी अधिनियम 2000 बनाया गया जिसके अंतर्गत किसी कंप्यूटर, कंप्यूटर प्रणाली या कंप्यूटर नेटवर्क प्रणाली के उल्लंघन के संबंध में नुकसान पहुंचाने के लिए शास्ति एवं प्रतिकर के लिए प्रावधान किए गए हैं। हालांकि भारत में अभी तक साइबर हमलों से निपटने के लिए अलग से कोई कानून अस्तित्व में नहीं है किंतु वर्तमान समय में सूचना प्रौद्योगिकी अधिनियम के अंतर्गत ही साइबर हमलों के विरुद्ध कार्यवाही होती है।

वैश्विक स्तर पर संयुक्त रूप से साइबर अपराध को रोकने के संबंध में बुडापेस्ट सम्मेलन पहला अंतरराष्ट्रीय सम्मेलन है। किंतु विश्व के दो मुख्य देश ब्राजील और भारत बुडापेस्ट संधि का हिस्सा नहीं है यदि साइबर हमलों से सुरक्षा के उपाय के संबंध में बात करें तो विश्व स्तर पर प्रत्येक देश को एक मंच पर आना होगा और साइबर हमलों से निपटने के लिए सही पहल करनी होगी।

हालांकि राष्ट्रीय एवं अंतर्राष्ट्रीय स्तर पर अनेक नियम, कानून एवं अभिसमय या सम्मेलन आदि हुए हैं तथा इन नियमों तथा कानूनों में उन्नयन भी किया जा रहा है, किंतु यह स्थिति और भी भयावह होती जा रही है और वर्तमान समय के नियम, कानून इस समस्या के सम्मुख बोने सिद्ध हो रहे हैं। इस अंतरराष्ट्रीय समस्या से निपटने के लिए जल्द ही वैश्विक स्तर पर एक साथ आना होगा।

जांच–परिणाम

- साइबर अपराध से संबंधित बढ़ते आंकड़े चिंताजनक विषय है यह मामले वर्ष दर वर्ष कई गुना वृद्धि कर रहे हैं जो साइबर क्रियाकलापों के लिए घातक सिद्ध हो सकते हैं,
- यह समस्या स्थानीय या देशीय नहीं बल्कि वैश्विक है किंतु साइबर सुरक्षा को लेकर वैश्विक भागीदारी की कमी,
- अंतरराष्ट्रीय स्तर पर संयुक्त रूप से साइबर सुरक्षा को लेकर नियमों की कमी,
- कंप्यूटर व मोबाइल विनिर्माण कंपनियों के द्वारा तकनीकी खामियां,
- लोगों में सोशल मीडिया को लेकर सतर्कता व जागरूकता की कमी

सुझाव

- संगणक या संगणक संजालों के उपयोगकर्ताओं को साइबर हमले व इसके दुरुपयोग से संबंधित विषयों की सामान्य जानकारी से अवगत कराना,
- कंप्यूटर , मोबाइल व अन्य प्रकार के अन्य यांत्रिक निर्मात्री संस्थाओं के लिए राष्ट्रीय एवं अंतर्राष्ट्रीय स्तर पर नियम बनाना जिससे वह अपनी तकनीकी को साइबर हमलेरोधी बना सके,
- लोगों को संजालों के प्रयोग में सतर्कता और सावधानी बरतना और अनजान साइट्स पर अनावश्यक विचरण न करना,
- सोशल मीडिया प्लेटफॉर्म के लिए मानक तैयार करना ताकि इससे जुड़े लोगों के डाटा को लीक न किया जा सके,

संदर्भ–सूची

1. https://en.wikipedia.org/wiki/Convention_on_Cybercrime#:~:text=The%20Convention%20on%20Cybercrime%2C%20also,and%20increasing%20cooperation%20among%20nations.
2. https://en.wikipedia.org/wiki/Cybercrime
3. https://cybervolunteer.mha.gov.in/webform/Volunteer_AuthoLogin.aspx
4. https://www.livemint.com/technology/tech-news/52-of-indian-firms-fell-victim-to-cyber-attack-in-last-12-months-sophos-survey-11617089719022.html
5. https://en.wikipedia.org/wiki/Social_media
6. https://www.amarujala.com/
7. https://pages.checkpoint.com/mobile-security-report-2021.html