Knowledgeable Research (An International Peer-Reviewed Multidisciplinary Journal) **ISSN 2583-6633**
Available Online: http://knowledgeableresearch.com Vol.03, No.5, December, 2024

भारत में साइबर अपराध के समाधान हेतु विधिक संरचना

नेहा सक्सेना
शोध छात्रा, विधि संकाय, मदरहुड विश्वविद्यालय, रूड़की, उत्तराखण्ड
डॉ. नलनीश चन्द्र सिंह
सह-आचार्य, विधि संकाय, मदरहुड विश्वविद्यालय, रूड़की, उत्तराखण्ड

****

*सारांशः- **21**वीं सदी इंटरनेट और प्रौद्योगिकी की सदी के रूप में जानी जाती है। इस समय में समाज का प्रत्येक व्यक्ति और संस्था कम्प्यूटर पर निर्भर है। इंटरनेट ने कम्प्यूटर की कार्यशैली को अप्रत्याशित रूप से प्रभावित किया है। साइबर अपराध के अन्तर्गत डेटा उल्लंघन और पहचान की चोरी से लेकर साइबर आतंकवाद और ऑनलाइन उत्पीड़न तक, साइबर अपराध में कई तरह की अवैध गतिविधियाँ शामिल हैं जो डिजिटल सिस्टम की कमजोरियों का फायदा उठाती हैं। प्रस्तुत शोध पत्र का उद्देश्य भारत में बढ़ती साइबर अपराध की समस्या की जटिलता का पता लगाना तथा इसके समाधान हेतु कानूनी प्रावधानों का अवलोकन कर इसके संबंध कानूनी प्रतिक्रियाओं को बढ़ाने के लिए सुझाव प्रस्तुत करना है। भारत में इंटरनेट के उपयोग में वृद्धि के साथ साइबर अपराध की वृद्धि दर भी बढ़ रही है। विधायी सुधार, अंतर्राष्ट्रीय सहयोग, क्षमता निर्माण, जन जागरूकता और नैतिक विचारों को शामिल करने वाले व्यापक दृष्टिकोण को अपनाकर, सरकारें साइबर खतरों से बेहतर तरीके से निपट सकती हैं और डिजिटल पारिस्थितिकी तंत्र की अखंडता की रक्षा कर सकती हैं।*

मुख्य शब्दः- *कम्प्यूटर, इंटरनेट, अपराध, साइबर अपराध, कानूनी प्रावधान*

****

प्रस्तावनाः-

21वीं सदी इंटरनेट और प्रौद्योगिकी की सदी के रूप में जानी जाती है। इस समय में समाज का प्रत्येक व्यक्ति और संस्था कम्प्यूटर पर निर्भर है चाहे वह किसी भी क्षेत्र- खेल, शिक्षा, रोजगार, मनोरंजन, आदि से जुड़ा हो। इंटरनेट ने कम्प्यूटर की कार्यशैली को अप्रत्याशित रूप से प्रभावित किया है। जिसने लोगों की कार्यकुशलता तथा अवसरों को भी बढ़ाया है। कई लोग इंटरनेट का प्रयोग सही कार्यों हेतु करते हैं तो कई लोग इसका प्रयोग गलत उद्देश्यों से अपने हित के लिए भी करते हैं जो इंटरनेट सम्बन्धी अपराधों को जन्म देता है। इन इंटरनेट सम्बन्धी अपराधों को साइबर अपराध की संज्ञा से अभिहीत किया गया। इस प्रकार यह क्षेत्र भी अपराध की दुनिया से अछूता नहीं रहा। साइबर अपराध जिसे ई-अपराध के रूप में भी जाना जाता है, को कम्प्यूटर से सम्बन्धित अपराध के रूप में परिभाषित किया जाता है। डिजिटल तकनीकों के प्रसार ने संचार, वाणिज्य और शासन में क्रांति ला दी है, लेकिन इसने साइबर अपराध के रूप में जानी जाने वाली आपराधिक गतिविधियों के नए रूपों को भी जन्म दिया है। डेटा उल्लंघन और पहचान की चोरी से लेकर साइबर आतंकवाद और ऑनलाइन उत्पीड़न तक, साइबर अपराध में कई तरह की अवैध गतिविधियाँ शामिल हैं जो डिजिटल सिस्टम की कमजोरियों का फायदा उठाती

हैं। इस संदर्भ में, साइबर खतरों से निपटने में मौजूदा कानूनों की पर्याप्तता एक गंभीर चिंता का विषय बन जाती है, जिसके लिए कानूनी ढाँचों और उनके सुधार के लिए रणनीतियों की व्यापक जाँच की आवश्यकता होती है।

सम्बन्धित साहित्य की समीक्षा:-

गिरि, डॉ. सविता आर. (2023)[1] ने अपने शोध पत्र 'भारत में साइबर अपराधों पर एक कानूनी अध्ययनः कानूनी ढाँचे को मजबूत करने के लिए मौजूदा कानूनों और रणनीतियों की पर्याप्तता का आकलन' में बताया कि सरकारें विधायी सुधार, अंतर्राष्ट्रीय सहयोग, क्षमता निर्माण, जन जागरूकता और नैतिक विचारों को शामिल करने वाले व्यापक दृष्टिकोण को अपनाकर, साइबर खतरों से बेहतर तरीके से निपट सकती हैं और डिजिटल पारिस्थितिकी तंत्र की अखंडता की रक्षा कर सकती हैं। **शर्मा, सुनीता कुमारी (2022)**[2] **ने**, 'ग्रामीण व शहरी शिक्षण प्रशिक्षणार्थियों की साइबर अपराध के प्रति जागरूकता का तुलनात्मक अध्ययन' नामक शीर्षक पर अध्ययन कार्य किया। अध्ययन निष्कर्ष में पाया गया कि ग्रामीण प्रशिक्षणार्थियों की जागरूकता का स्तर कम है वहीं शहरी प्रशिक्षणार्थियों की जागरूकता का स्तर ज्यादा है। **भांगला, अपूर्वा एवं तुली, जानवी (2021)**[3] **ने,** 'A Study on Cyber Crime and its Legal Framework in India' विषय पर शोधपत्र प्रकाशित किया। साइबर-अपराध में मुख्य रूप से ऐसी गतिविधियाँ शामिल हैं जो किसी व्यक्ति की निजी जानकारी को प्रत्यक्ष या अप्रत्यक्ष रूप से निकालने के लिए एक उपकरण के रूप में इंटरनेट और कंप्यूटर का उपयोग करती हैं और व्यक्ति की सहमति के बिना या अवैध रूप से प्रतिष्ठा को कम करने या मानसिक या शारीरिक नुकसान पहुंचाने के उद्देश्य से इसे ऑनलाइन प्लेटफार्म पर प्रकट करती हैं। **अलगाम्दी, मोहम्मद आई. (2020)**[4] **ने,** 'A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide' विषय पर शोध पत्र प्रकाशित किया। शोध में अनुमान लगाया गया था कि साइबर अपराधियों के हाथों प्रति वर्ष छह ट्रिलियन डॉलर तक का नुकसान हो सकता है।

[1] Dr. Sarvita R. Giri (2023). 'A Legal Study on Cybercrimes in India: Assessing the Adequacy of Present Laws and Strategies for Strengthening Legal Frameworks'. *Social Sciecne Journal,* 13(4). 372-378. https://resmilitaris.net/uploads/paper/09e503807f4a471a7fa036ab1820121f.pdf

[2] शर्मा, सुनीता कुमारी (2022), ''ग्रामीण व शहरी शिक्षण प्रशिक्षणार्थियों की साइबर अपराध के प्रति जागरूकता का तुलनात्मक अध्ययन'' *International Journal of Creative Research Thoughts*, Vol. 10, Issue.5, pp: 19-22. https://ijcrt.org/papers/IJCRTP020004.pdf

[3] Bhangla, Apoorva & Tuli, Jahanvi (2021), "A Study on Cyber Crime and its Legal Framework in India", *Intenrational Journal of Law Management & Humanities*, Vol.4, Issue.2, pp: 493-504. https://www.ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/

[4] Alghamdi, Mohammed I. (2020), "A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide", *International Journal of Engineering Research & Technology*, Vol.9, Issue.6, pp: 731-735. https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide

अध्ययन के उद्देश्य:-

- साइबर अपराध की अवधारणा, अर्थ एवं प्रकारों का अध्ययन करना।
- भारत में साइबर अपराध की बढ़ती समस्याओं का अध्ययन करना।
- साइबर अपराधों से निबटने हेतु भारत में किये गये कानूनी प्रावधानों की चर्चा करना।

साइबर अपराध एवं इसके प्रकार:-

जब हम किसी को जानबूझकर चोट पहुँचाते हैं या किसी का कोई सामान बिना इजाजत के लेते हैं तो यह कृत्य अपराध कहलाता है। सुसमैन और हेस्टन ने पहली बार वर्ष 1995 में 'साइबर अपराध' शब्द का प्रयोग किया था।

साइबर अपराध की परिभाषा:-

साइबर अपराध को इस प्रकार परिभाषित किया जा सकता है, ''अपराध जो जानबूझकर पीड़ित की प्रतिष्ठा को नुकसान पहुंचाने या आधुनिक दूरसंचार नेटवर्क का उपयोग करके प्रत्यक्ष या अप्रत्यक्ष रूप से पीड़ित को शारीरिक या मानसिक नुकसान पहुंचाने के लिए आपराधिक इरादे से व्यक्तियों या व्यक्तियों के समूहों के खिलाफ किए जाते हैं-जैसे इंटरनेट (चैट रूम, ईमेल, नोटिस बोर्ड) और मोबाइल फोन।''

साइबर अपराध में इंटरनेट और कंप्यूटर का उपयोग शामिल है। यह किसी व्यक्ति की प्रतिष्ठा को कम करने और उन्हें प्रत्यक्ष या अप्रत्यक्ष रूप से शारीरिक या मानसिक नुकसान पहुंचाने के उद्देश्य से उनकी व्यक्तिगत या गोपनीय जानकारी को ऑनलाइन प्रकट या प्रकाशित करके उनकी गोपनीयता को खतरे में डालता है। साइबर अपराध दुनिया भर के लोगों के लिए खतरा बनता जा रहा है।

साइबर अपराध के प्रकार:-

साइबर अपराध में कंप्यूटर और इंटरनेट का उपयोग करके की जाने वाली कई तरह की अवैध गतिविधियाँ शामिल हैं। यहाँ साइबर अपराधों के कुछ सामान्य प्रकार निम्नवत् हैं-

1. **हैकिंग -** हैकिंग एक ऐसा कार्य है जो धोखेबाज द्वारा दूसरों के कंप्यूटर सिस्टम को उनकी अनुमति के बिना पढ़कर किया जाता है। हैकर कंप्यूटर प्रोग्रामर होते हैं, जिन्हें कंप्यूटर की नवीन समझ होती है और वे आमतौर पर धोखेबाजी के लिए इस ज्ञान का दुरुपयोग करते हैं। उनके पास किसी विशेष प्रोग्राम या भाषा में अतिरिक्त कौशल होता है और वे इंटरनेट स्पेस में माहिर होते हैं। एक हैकर व्यक्तिगत बैंकिंग जानकारी, किसी निगम का वित्तीय डेटा आदि चुराने के लिए सिस्टम में सेंध लगाता है। वे सिस्टम को बदलने की भी कोशिश करते हैं ताकि वे अपने मनचाहे काम पूरे कर सकें। इन लोगों को ब्लैक हैट कहा जाता है।
2. **साइबर स्टाकिंग:-** साइबर स्टाकिंग का अर्थ है किसी व्यक्ति द्वारा किसी व्यक्ति का पीछा करने के लिए इलेक्ट्रॉनिक संचार का उपयोग करना, या किसी व्यक्ति द्वारा स्पष्ट रूप से अरुचि के संकेत के बावजूद बार-बार

व्यक्तिगत संपर्क को बढ़ावा देने के लिए उससे संपर्क करने का प्रयास करनाय या इंटरनेट, ईमेल या इलेक्ट्रॉनिक संचार के किसी अन्य रूप पर नजर रखना, स्टॉकिंग का अपराध है।

3. **साइबर बुलिंग:-** साइबरबुलिंग में कंप्यूटर, टैबलेट, लैपटॉप और सेल फोन जैसे डिजिटल उपकरणों पर हानिकारक या झूठी सामग्री भेजकर, पोस्ट करके या साझा करके किसी के व्यक्तिगत के निजी डेटा को साझा करके शर्मिंदगी या अपमान पैदा करने के लिए इंटरनेट का उपयोग शामिल है। यह एसएमएस, ऑनलाइन गेमिंग समूहों, ऑनलाइन फोरम या सोशल मीडिया प्लेटफार्म के माध्यम से हो सकता है जहां जानकारी का ऑनलाइन आदान-प्रदान किया जा सकता है और कई लोगों के लिए उपलब्ध है। साइबरबुलिंग निरंतर और स्थायी है और इसलिए, न केवल पीड़ित बल्कि इसमें शामिल दोनों पक्षों की ऑनलाइन प्रतिष्ठा को नुकसान पहुंचा सकता है।
4. **साइबर मॉर्फिंग:-** यह एक प्रकार का अपराध है जिसमें मूल तस्वीर को किसी अनधिकृत उपयोगकर्ता या नकली पहचान रखने वाले व्यक्ति द्वारा संपादित किया जाता है। महिला उपयोगकर्ताओं की तस्वीरें उनकी प्रोफाइल से ली जाती हैं और फिर उन्हें संपादित करने के बाद विभिन्न साइटों पर नकली खातों द्वारा अश्लील उद्देश्यों के लिए दोबारा पोस्ट किया जाता है।
5. **ई-मेल स्पूफिंग:-** यह सबसे आम साइबर क्राइम में से एक है। इसमें ई-मेल भेजना शामिल है जो इसके मूल का प्रतिनिधित्व करता है। आज के समय में यह अपराध इतना आम हो गया है कि यह आकलन करना बहुत मुश्किल हो जाता है कि जो मेल प्राप्त हुआ है वह वास्तव में मूल प्रेषक का है या नहीं। ईमेल स्पूफिंग का इस्तेमाल ज्यादातर महिलाओं से धोखाधड़ी से निजी जानकारी और निजी तस्वीरें निकालने के लिए किया जाता है और बाद में उन्हें ब्लैकमेल करने के लिए किया जाता है।
6. **फिशिंग:-** फिशिंग उपयोगकर्ता नाम और पासवर्ड जैसी संवेदनशील जानकारी प्राप्त करने का प्रयास है और व्यक्तिगत जानकारी प्राप्त करने का इरादा है।
7. **ट्रोलिंग:-** यह सोशल मीडिया प्लेटफार्म पर ऑनलाइन हिंसा का एक रूप है जहां लोगों को अपनी बात कहने की आजादी दी जाती है। ऑनलाइन उत्पीड़क अक्सर उन लोगों को निशाना बनाते हैं जो अपनी राय व्यक्त करते हैं और प्रचलित सामाजिक मानदंडों से अलग सोचते हैं। ऐसे वर्ग में महिलाएं शामिल हैं, जिन्हें सोशल मीडिया बदमाशों द्वारा निशाना बनाया जाता है।
8. **डेबिट/क्रेडिट कार्ड धोखाधड़ी:-** क्रेडिट कार्ड (या डेबिट कार्ड) धोखाधड़ी में खरीदारी या उससे धन निकालने के उद्देश्य से किसी अन्य व्यक्ति के क्रेडिट या डेबिट कार्ड की जानकारी का अनधिकृत उपयोग शामिल होता है।

इसके अलावा साइबर अपराधों में डाटा ब्रीच, वेबसाइट डिफेसमेंट, विसिंग आदि सम्मिलित हैं।

भारत में साइबर अपराधों की बढ़ती समस्या:-

दुनिया तथा भारत में बढ़ते हुए साइबर अपराधों पर नजर डाले तो पता चलता है कि जनवरी से अप्रैल 2024 के बीच साइबर अपराध की वजह से भारतीय नागरिकों को 1,750 करोड़ रुपये से ज्यादा का नुकसान हुआ है। इकोनॉमिक टाइम्स की एक रिपोर्ट के अनुसार, भारतीय साइबर अपराध समन्वय केंद्र ने कहा कि मई 2024 में प्रतिदिन औसतन 7,000 साइबर अपराध शिकायतें दर्ज की गईं, जो 2021 और 2023 के बीच की अवधि की तुलना में 113.7 प्रतिशत की उल्लेखनीय वृद्धि और 2022 से 2023 तक 60.9 प्रतिशत की वृद्धि को दर्शाता है। भारतीय साइबर अपराध समन्वय केन्द्र में वर्ष 2019 से 2024 तक दर्ज मामलों में अधिकांश पीड़ित ऑनलाइन निवेश धोखाधड़ी, गेमिंग ऐप, एल्गोरिदम हेरफेर, अवैध ऋण ऐप, सेक्सऑर्शन और ओटीपी घोटाले के शिकार हुए। 2023 में, भारतीय साइबर अपराध समन्वय केन्द्र ने 100,000 से अधिक निवेश धोखाधड़ी की घटनाओं की सूचना दी। 2024 के शुरुआती चार महीनों में डिजिटल गिरफ्तारियों के कारण 4,599 मामलों में 120 करोड़ रुपये का नुकसान हुआ। ट्रेडिंग घोटालों के 20,043 मामले सामने आए, जिससे इसी अवधि के दौरान साइबर अपराधियों को 1,420 करोड़ रुपये का नुकसान हुआ। भारतीय साइबर अपराध समन्वय केन्द के आंकड़ों के अनुसार, निवेश घोटालों के कारण 62,687 शिकायतों में 222 करोड़ रुपये का नुकसान हुआ, जबकि डेटिंग ऐप्स के कारण 1,725 शिकायतों में 13.23 करोड़ रुपये का नुकसान हुआ। जनवरी से अप्रैल 2024 तक भारतीयों पर साइबर अपराधियों द्वारा लगाया गया कुल वित्तीय नुकसान 176 करोड़ रुपये तक पहुँच गया।

इस प्रकार वर्तमान में साइबर अपराध एक विकराल समस्या बन चुकी है। इसके समाधान हेतु ठोस कदम नहीं उठाये गये तो यह आम जन को बूरी तरह प्रभावित ही करेगा साथ ही विभिन्न संस्थाओं- जैसे- बैंक, सरकारी संस्थाओं आदि के लिए भी घातक साबित होगा। हालांकि भारत सरकार द्वारा इससे निबटने के लिए समय-समय उचित कदम उठाये हैं। सरकार द्वारा साइबर अपराध को रोकने हेतु जो कानूनी कदम उठाये गये हैं उनमें से प्रमुख प्रावधनों को शोधार्थी द्वारा वर्णित किया जा रहा है।

भारत में साइबर अपराध के समाधान हेतु किये गये कानूनी प्रावधान:-

साइबर अपराधी लगातार अपनी रणनीति बदलते रहते हैं, जिससे व्यक्तियों और संगठनों के लिए सतर्क रहना और मजबूत साइबर सुरक्षा उपाय अपनाना जरूरी हो जाता है। भारत में, साइबर अपराध और साइबर सुरक्षा से जुड़े कई कानून और अधिनियम हैं। यहाँ कुछ मुख्य कानून दिए गए हैं:-

1. **सूचना प्रौद्योगिकी अधिनियम, 2000 (आईटी अधिनियम):-** आईटी अधिनियम भारत में साइबर गतिविधियों को नियंत्रित करने वाला प्राथमिक कानून है। यह इलेक्ट्रॉनिक लेनदेन को कानूनी मान्यता प्रदान करता है, ई-गवर्नेंस की सुविधा प्रदान करता है, और साइबर अपराध और साइबर सुरक्षा से निपटता है। धारा

43, 66, 66A, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 70, और अन्य साइबर अपराधों के लिए प्रासंगिक हैं।

2. **भारतीय दंड संहिता (IPC):-** साइबर अपराधों के लिए विशिष्ट नहीं होने पर भी, प्च्ब् की कई धाराएँ साइबर अपराधों पर लागू होती हैं, जैसे धोखाधड़ी, मानहानि, पहचान की चोरी और जबरन वसूली से संबंधित धाराएँ।
3. **सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008:-** इस संशोधन अधिनियम ने आईटी अधिनियम के दायरे का विस्तार किया और साइबर अपराधों से संबंधित नए प्रावधान पेश किए, जिनमें डेटा सुरक्षा, साइबर आतंकवाद और कुछ अपराधों के लिए दंड शामिल हैं।
4. **आधार (वित्तीय और अन्य सब्सिडी, लाभ और सेवाओं का लक्षित वितरण) अधिनियम, 2016:-** यह अधिनियम भारत की बायोमेट्रिक पहचान प्रणाली आधार के उपयोग और सुरक्षा को नियंत्रित करता है, और इसमें व्यक्तिगत डेटा और गोपनीयता की सुरक्षा से संबंधित प्रावधान शामिल हैं।
5. **भुगतान और निपटान प्रणाली अधिनियम, 2007:-** यह अधिनियम भुगतान प्रणालियों को नियंत्रित करता है और इलेक्ट्रॉनिक भुगतान लेनदेन की सुरक्षा और संरक्षण प्रदान करता है।
6. **भारतीय रिजर्व बैंक (RBI) विनियम:-** RBI साइबर खतरों से बचाने के लिए बैंकिंग और वित्तीय क्षेत्र में साइबर सुरक्षा से संबंधित विभिन्न विनियम और दिशानिर्देश जारी करता है।
7. **राष्ट्रीय साइबर सुरक्षा नीति, 2013:-** हालांकि यह स्वयं एक कानून नहीं है, लेकिन यह नीति भारत में साइबर सुरक्षा चुनौतियों का समाधान करने के लिए एक रूपरेखा प्रदान करती है और साइबर सुरक्षा बुनियादी ढांचे और क्षमताओं को बढ़ाने के लिए रणनीतियों की रूपरेखा तैयार करती है।
8. **व्यक्तिगत डेटा संरक्षण विधेयक, 2019 (पीडीपी विधेयक):-** हालांकि मेरे अंतिम अपडेट के अनुसार इसे अधिनियमित नहीं किया गया है, लेकिन इस विधेयक का उद्देश्य व्यक्तिगत डेटा के प्रसंस्करण को विनियमित करना और वैश्विक मानकों के अनुरूप डेटा सुरक्षा ढांचा स्थापित करना है।
9. **डिजिटल पर्सनल डाटा प्रोटेक्शन अधिनियम, 2023:-** अधिनियम का मुख्य उद्देश्य डिजिटल व्यक्तिगत डेटा के प्रसंस्करण और सुरक्षा के लिए एक संरचना प्रदान करना है। यह भारत के भीतर और बाहर दोनों जगह लागू है (बशर्ते कि भारत के नागरिकों का डिजिटल डेटा संदिग्ध हो)। यह भारत में अन्य नियमध्कानून बनाने के लिए आधार भी निर्धारित करता है, जैसे डिजिटल इंडिया अधिनियम और व्यवसाय/उद्योग-विशिष्ट डेटा सुरक्षा और गोपनीयता विनियम।

ये भारत में साइबर अपराध और साइबर सुरक्षा से संबंधित कुछ प्रमुख कानून और अधिनियम हैं। अनुपालन सुनिश्चित करने और साइबर खतरों से प्रभावी ढंग से निपटने के लिए इन कानूनों में किसी भी संशोधन या परिवर्धन पर अपडेट रहना महत्वपूर्ण है।

श्रेया सिंघल बनाम भारत संघ[5] में, पांच साल पहले तय, सुप्रीम कोर्ट ने निष्कर्ष निकाला कि मुद्दे पर पूरा खंड एक्स्ट्रा वायर्स था क्योंकि यह अनुच्छेद 19 (1) (ए) का उल्लंघन करता था और अनुच्छेद 19(2) द्वारा संरक्षित नहीं था। परिणामस्वरूप, आईटी अधिनियम की धारा 66 ए के तहत कोई एफआईआर दर्ज नहीं की जानी चाहिए थी। अपील में राज्य कानून प्रवर्तन अधिकारियों और यहां तक कि न्यायपालिका के निचले स्तर पर भी श्रेया सिंघल निर्णय के निरंतर उपयोग की ओर ध्यान आकर्षित किया गया है, जो निर्णय के बारे में पूरी तरह से जानकारी के अभाव के कारण हो सकता है। यह विनियमन पुलिस अधिकारियों और न्यायाधीशों सहित सभी पर लागू होता है।

मोहन सिंह बनाम उत्तर प्रदेश राज्य[6] में इलाहाबाद उच्च न्यायालय की खंडपीठ ने वरिष्ठ पुलिस अधीक्षक को एक व्यक्तिगत बयान देने का आदेश दिया, जिसमें यह स्पष्टीकरण दिया गया कि आईटी (संशोधन) अधिनियम, 2008 की धारा 66 ए के तहत प्राथमिकी कैसे दर्ज की गई थी। याचिकाकर्ता ने दावा किया कि आईटी अधिनियम के प्रावधान 66 ए और 67 बी और भारतीय रदंड संहिता की धारा 294, 500, 504, 506 और 509 का उपयोग वर्तमान एफआईआर (आईपीसी) में आरोपियों के खिलाफ मुकदमा चलाने के लिए किया गया था।

सिटिंग इरोस बनाम बीएसएनएल[7] **और डिपार्टमेंट ऑफ इलेक्ट्रानिक्स एण्ड इनफॉर्मेशन टेक्नोलॉजी (DEITY) बनाम स्टार इंडिया**[8] में, न्यायालय ने नोट किया कि ''दुष्ट वेबसाइट'' की पहचान करने की सीमा मात्रात्मक के बजाय गुणात्मक होनी चाहिए। ये वेबसाइटें निषेधाज्ञा से बचने के लिए वैध सामग्री की थोड़ी मात्रा अपलोड करेंगी, यदि केवल उल्लंघनकारी सामग्री वाली वेबसाइटें दुर्भावनापूर्ण मानी जाती हैं (यानी, मात्रात्मक दृष्टिकोण)। अदालत ने यह माना कि ये वेबसाइटें कानूनी अधिकारों का घोर उल्लंघन कर रही हैं, इसलिए इन वेबसाइटों पर सम्पूर्ण प्रतिबंध लगाने का कठोर कदम उठाना सर्वप्रथम उचित था।

श्रीकुमार बनाम केरल राज्य[9] मामल में, केरल उच्च न्यायालय ने एक राजनीतिक दल की महिला सदस्य के फेसबुक पेज पर अपमानजनक टिप्पणियां पोस्ट करने से संबंधित मामले पर विचार किया।

इस प्रकार साइबर अपराध से सम्बन्धित कई मामले भारत के न्यायालयों में निर्णित किये गये हैं जो बढ़ते साइबर अपराध को उजागर करते हैं। साइबर अपराधों को संबोधित करने

[5] (2013) 12 SCC 73
[6] 2020 SCC OnLine All 920, decided on 31.07.2020.
[7] 2016 SCC OnLineBom 10315 (Single Judge Bench)
[8] HC of Delhi (Division Bench) FAO(OS) 57/2015.
[9] SCC OnLine Ker 1305, (Order Date, 03.04.2019).

और साइबर सुरक्षा सुनिश्चित करने के लिए कानून, प्रौद्योगिकी, शिक्षा और अंतर्राष्ट्रीय सहयोग से जुड़े बहुआयामी दृष्टिकोण की आवश्यकता होती है। साइबर कानूनों को बेहतर बनाने और साइबर अपराधों से निपटने के लिए निम्न सुझावों को दृष्टिगत किया जा सकता है-

1. **व्यापक कानून**: विकसित होती तकनीक और उभरते साइबर खतरों के साथ तालमेल बनाए रखने के लिए साइबर कानूनों को लगातार अपडेट और मजबूत करें। सुनिश्चित करें कि कानून हैकिंग, पहचान की चोरी, फिशिंग, मैलवेयर और साइबरबुलिंग सहित साइबर अपराधों की एक विस्तृत श्रृंखला को कवर करते हैं।
2. **अंतर्राष्ट्रीय सहयोग**: राष्ट्रीय सीमाओं को पार करने वाले साइबर अपराधों को संबोधित करने के लिए देशों के बीच सहयोग और सूचना साझाकरण को बढ़ावा दें। साइबर सुरक्षा और साइबर अपराध से संबंधित अंतर्राष्ट्रीय समझौतों और सम्मेलनों, जैसे कि साइबर अपराध पर बुडापेस्ट कन्वेंशन की पुष्टि करें और उन्हें लागू करें।
3. **क्षमता निर्माण और प्रशिक्षण**: साइबर अपराधों को प्रभावी ढंग से संभालने में कानून प्रवर्तन एजेंसियों, न्यायपालिका और कानूनी पेशेवरों की क्षमता का निर्माण करने के लिए प्रशिक्षण कार्यक्रमों में निवेश करें। डिजिटल फोरेंसिक, साइबर जांच और साइबर कानून प्रवर्तन में विशेष प्रशिक्षण प्रदान करें।
4. **सार्वजनिक जागरूकता और शिक्षा**: साइबर सुरक्षा जोखिमों और सुरक्षित ऑनलाइन व्यवहार के लिए सर्वोत्तम प्रथाओं के बारे में आम जनता के बीच जागरूकता बढ़ाएँ। व्यक्तियों को सामान्य साइबर खतरों, जैसे कि फिशिंग, मैलवेयर और पहचान की चोरी, और साइबर अपराधों से खुद को कैसे सुरक्षित रखें, के बारे में शिक्षित करें।
5. **साइबर सुरक्षा अवसंरचना**: मजबूत साइबर सुरक्षा ढांचे, घटना प्रतिक्रिया क्षमताओं और साइबर रक्षा तंत्र में निवेश करके राष्ट्रीय स्तर पर साइबर सुरक्षा अवसंरचना को मजबूत करें। महत्वपूर्ण अवसंरचना क्षेत्रों के लिए साइबर सुरक्षा मानकों और दिशानिर्देशों को विकसित और लागू करें।
6. **डेटा सुरक्षा और गोपनीयता विनियम**: व्यक्तिगत डेटा और संवेदनशील जानकारी को अनधिकृत पहुँच, प्रकटीकरण और दुरुपयोग से बचाने के लिए व्यापक डेटा सुरक्षा और गोपनीयता कानून लागू करें। अंतर्राष्ट्रीय डेटा सुरक्षा मानकों, जैसे कि सामान्य डेटा सुरक्षा विनियमन (ळक्च्त्) का अनुपालन सुनिश्चित करें।

इन समाधानों को लागू करके, सरकारें साइबर कानूनों को मजबूत कर सकती हैं, साइबर सुरक्षा क्षमताओं को बढ़ा सकती हैं, और तेजी से डिजिटल होती दुनिया में साइबर अपराधों से जुड़े जोखिमों को कम कर सकती हैं।

निष्कर्ष:-

यह शोध पत्र साइबर अपराधों से निपटने में वर्तमान कानूनों की पर्याप्तता का आकलन करने के महत्व को रेखांकित करता है और डिजिटल युग की उभरती चुनौतियों का सामना करने के लिए कानूनी ढाँचे को मजबूत करने की रणनीतियों का प्रस्ताव करता है। निष्कर्ष रूप में कहा जाये तो भारत में इंटरनेट के उपयोग में वृद्धि के साथ साइबर अपराध की वृद्धि दर भी बढ़ रही है। साइबर अपराधों के उभरते प्रकार वे अपराध हैं जो बार-बार नहीं होते बल्कि नए होते हैं। इस प्रकार के अपराध बिना किसी पूर्व संकेत के होते हैं। कंप्यूटर का उपयोग करके अपराध जैसे हैकिंग, धमकी भरी जानकारी प्रकाशित करना, धोखाधड़ी करना, चोरी किए गए संचार उपकरण या कंप्यूटर प्राप्त करना, साइबर आतंकवाद, दूसरों की निजी छवियों को प्रकाशित करना, अश्लील जानकारी प्रकाशित करना, यौन कृत्यों वाली छवियों को प्रकाशित करना, बाल पोर्नोग्राफी, पहचान की चोरी, धोखाधड़ी और क्रेडिट/डेबिट कार्ड धोखाधड़ी जैसे अपराध बहुत अधिक दर पर सामने आए हैं। ऐसे अपराधों से निपटने के लिए, भारत सरकार और साइबर अधिकारियों को अपडेट रहने और किसी भी वर्ष में किसी भी समय किसी भी नए उभरते अपराध से निपटने के लिए खुद को तैयार रखने की आवश्यकता है। विधायी सुधार, अंतर्राष्ट्रीय सहयोग, क्षमता निर्माण, जन जागरूकता और नैतिक विचारों को शामिल करने वाले व्यापक दृष्टिकोण को अपनाकर, सरकारें साइबर खतरों से बेहतर तरीके से निपट सकती हैं और डिजिटल पारिस्थितिकी तंत्र की अखंडता की रक्षा कर सकती हैं। जैसे-जैसे साइबर अपराध बढ़ रहे हैं, भारत सरकार भी समाचार पत्रों में लेख, रेडियो और टेलीविजन पर विज्ञापन प्रकाशित करके, सुरक्षित रहने के लिए ईमेल और पाठ संदेश भेजकर, अपराध की रिपोर्ट करने के लिए कई मोबाइल एप्लिकेशन और वेबसाइटें उपलब्ध कराकर और सोशल नेटवर्किंग साइबर जागरूकता और रिपोर्टिंग पोर्टल के माध्यम से प्रत्येक इंटरनेट उपयोगकर्ता तक पहुंचकर विभिन्न जागरूकता और रोकथाम के उपाय कर रही है।

सुझाव:-

अध्ययन के विश्लेषण के आधार पर कहा जा सकता है कि सरकारों को उभरते साइबर खतरों से प्रभावी ढंग से निपटने के लिए मौजूदा कानूनों को अद्यतन और सुसंगत बनाने के लिए विधायी सुधारों को प्राथमिकता देनी चाहिए। साइबर अपराधों से निपटने में सीमा पार सहयोग को सुविधाजनक बनाने के लिए अंतर्राष्ट्रीय सहयोग तंत्र को मजबूत किया जाना चाहिए। साइबर खतरों के खिलाफ लचीलापन बढ़ाने के लिए क्षमता निर्माण, साइबर सुरक्षा शिक्षा और जन जागरूकता अभियानों में निवेश बढ़ाया जाना चाहिए तथा साइबर अपराधों से निपटने में सरकारों, उद्योग हितधारकों और नागरिक समाज संगठनों के बीच सहयोग को बढ़ावा देने के लिए सार्वजनिक-निजी भागीदारी को बढ़ावा दिया जाना चाहिए।

संदर्भ ग्रंथ सूची:-

1. भारत का संविधान, 1950।
2. सूचना प्रौद्योगिकी अधिनियम, 2000
3. भारतीय दण्ड संहिता, 1860।

4. परांजपे डॉ. एन.वी., विधि शास्त्र एवं विधि के सिद्धान्त सी.एल.ए. 18वां संस्करण, 2017
5. मिश्र, डॉ. जय प्रकाश, साइबर विधि एक परिचय, इलाहाबाद: सेंट्रल लॉ पब्लिकेशन।
6. Verma, Dr. Amit, *Cyber Crimes in India*, Allahabad: Central Law Publication, Ist Ed. 2012.
7. Debarati Haldar and K. Jaishankar, Cyber Crimes against Women in India, New Delhi: SAGE Publications India Ptv. Ltd., 2017.
8. https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html
9. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
10. https://lddashboard.legislative.gov.in/sites/default/files/A2007-51_0.pdf

Corresponding Author: Neha Saxena
E-mail: imadvneha@gmail.com
Received: 11 December, 2024; Accepted: 20 December, 2024. Available online: 30 December, 2024
Published by SAFE. (Society for Academic Facilitation and Extension)