IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

भारत में साइबर अपराध : एक अनुभवजन्य अध्ययन

डॉ. प्रतिमा रायकवार सोनी
सहायक प्राध्यापक एवं विभागाध्यक्ष
चित्रकला विभाग
श्री कृष्णाजीराव पवार शासकीय
स्नातकोत्तर महाविद्यालय, देवास (म.प्र.)

डॉ. प्रेमलता चौहान
सहायक प्राध्यापक (प्राणीशास्त्र)
श्री तुकोजीराव पवार शासकीय विज्ञान
स्नातकोत्तर महाविद्यालय, देवास (म.प्र.)

1) शोधसार (Abstract) :–

साइबर अपराध :– जब हम किसी को जानबुझकर शारीरिक चोट पहुंचते है या किसी का कुछ सामान बिना इजाजत लेते है तो यह अपराध कहलाता है। खून करना, चोरी या बैंक डकैती भी साइबर अपराध में भी है, पर तरीका बदल गया है। यहां हम किसी के कम्प्यूटर को या इसके डाटा को इंटरनेट के जरिये दुनिया में कहीं भी नुकसान पहुंचाते है, उसे साइबर अपराध के नाम से जाना जाता है। साइबर अपराध साधारणतः किसी प्रकार की हिंसा नही फैलाते लेकिन लालच, सम्मान और किसी व्यक्ति के चरित्र के कमजोर पहलू के साथ खेल कर विभिन्न अपराधों को जन्म देते है। साइबर अपराधों में आपराधिक गतिविधियां जैसे चोरी, धोखा, गबन, अपमान करना आदि सम्मिलित है। साइबर अपराध वे गैरकानूनी कार्य हैं, जिसमें कम्प्यूटर का इस्तेमाल होता है तथा इस में सूचना, तकनीकी एवं आपराधिक गतिविधियां सम्मिलित होती है।

- **व्यक्तिगत अपराध** : इस प्रकार के अपराध किसी व्यक्ति या उस की निजी संपत्ति आदि को ले कर हो सकते हैं। इनमें इलेक्ट्रॉनिक मेल, साइबर स्टाकिंग, अश्लील/आपत्तिजनक सामग्री के इंटरनेट द्वारा प्रसार से हैंकिंग/क्रैकिंग या किसी अन्य अपराध में कम्प्यूटर का प्रयोग करना, वायरस फैलाना, इंटरनेट साइट्स पर अतिक्रमण तथा बिना स्वीकृति के किसी व्यक्ति के कम्प्यूटर पर गलत या आपराधिक तरीके के कब्जा करना आदि सम्मिलित हैं।
- **किसी संस्था के विरूद्ध :–** इस प्रकार के अपराध सामान्यतः किसी सरकारी, निजी संस्था, कंपनी या किसी समूह के खिलाफ हो सकते हैं। ये अपराध भी हैंकिंग, क्रैकिंग

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

द्वारा अथवा गैरकानूनी ढंग से सूचनाओं को प्राप्त करने और उन का इस्तेमाल किसी संस्था या सरकार के विरूद्ध कर के किए जाते है। पाइरेटेड सॉफ्टवेयर का वितरण एवं अन्य प्रकार के गैरकानूनी कम्प्यूटर संबंधी कार्यो से संबंधित अपराध इस श्रेणी में अते है।

- **समाज के विरूद्ध** :– ये अपराध किसी व्यक्ति या संस्था के विरूद्ध की सीमित न रह कर संपूर्ण समाज को प्रभावित करते हैं। इस प्रकार के अपराधों में पोर्नोग्राफी तथा अश्लील सामग्री या ट्रैफिकिंग जैसे अपराध शामिल होते हैं।

प्रमुख साइबर अपराध :–

- **हैंकिंग** :– सूचना प्रौद्योगिकी ऐक्ट 2000 में इस प्रकार के अपराधों को बताते हुए कहा गया है, ''जो भी जानबूझ कर या बिना जाने किसी गलत कार्य द्वारा पब्लिक या व्यक्ति को हानि पहुंचाता है अथवा पहुंचाने का प्रयास करता है उसे हैंकिंग कहते है। इस प्रकार के अपराधों में कम्प्यूटर पर ही सूचना को गैरकानूनी ढंग से अधिगृहित कर नुकसान पहुंचाया जाता हैं।
- **सुरक्षा से संबंधित अपराध** :– इंटरनेट तथा नेटवर्क की तेज रफ्तार में वृद्धि के साथ नेटवर्क बहुत महत्वपूर्ण हो गई है, निजी गुप्त सूचनाओं को आमजन तथा प्रचारित–प्रसारित करना ही सुरक्षा व्यवस्था से संबंधित अपराधों की श्रेणी में आता है। यह कार्य नेटवर्क पौकेट स्निफर द्वारा किया जा सकता है, जो संपूर्ण सूचनाओं को छोटे–छोटे टुकड़ों में बांट कर उन का पुनः वितरण और प्रचार–प्रसार करते है। ये नेटवर्क पौकेट स्निफर एक साफ्टवेयर तकनीक को विकसित करते हैं तथा उपभोकर्ता को उपयोगी सूचनाएं ग्रहण करने हेतु खाता संख्या एवं पासवर्ड उपलब्ध करवाते हैं। सुरक्षा व्यवस्था को इस गंभीर खतरा उत्पन्न होता हैं।
- **इंटरनेट पर धोखाधड़ी** :– यह भी विशेष प्रकार का अपराध है। इंटरनेट कंपनियां इंटरनेट पर अपने उत्पादों की मार्केटिंग करती है। खराब उत्पादों की मार्केटिंग के लिए वे अपने ग्राहकों को गलत सूचनाएं दे कर उन्हें फंसाती है। यह सभी इंटरनेट धोखाधड़ी के अंतर्गत आता हैं।

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

- **क्रेडिट कार्ड धोखाधड़ी** :– इंटरनेट द्वारा मृदा का स्थानांतरण और लेनदेन करना बहुत आसान हो गया है, वहीं इस तकनीक ने कई प्रकार के साइबर अपराधों को जन्म भी दिया है। इनमें मुख्य है, क्रेडिट कार्ड धोखाधड़ी, इस प्रकार के अपराध में किसी कार्डधारक के डिजिटल हस्ताक्षर बना कर उस के कोड नंबर की चोरी की जाती है। भारतीय सूचना प्रौद्योगिकी ऐक्ट 2000 की धारा 73 के अनुसार इस प्रकार के अपराधों के लिए 2 वर्ष तक का कारावास या 2 लाख रूपए जुर्माना अथवा दोनों दंड निर्धारित हैं।
- **पोर्नोग्राफी** :– सूचना प्रौद्योगिकी अधिनियम 2000 के अनुसार अश्लील दृश्यों का प्रचार–प्रसार एक दंडनीय साइबर अपराध है। इस ऐक्ट के अनुसार जो भी व्यक्ति, संस्था या समूह किसी भी प्रकार की अश्लील सामग्री को प्रकाशित व प्रसारित करने का प्रयास करेगा, जिससे कि किसी व्यक्ति को पढ़ने, सुनने, देखने के लिए प्रेरित किया जा सके अथवा उस के मस्तिष्क में किसी प्रकार की विकृति उत्पन्न कर सके, को इस ऐक्ट के तहत साइबर अपराधी माना जाएगा। उसे 5 वर्ष की कैद या 1 लाख रूपए तक का जुर्माना अथवा दोनों सजा का प्रावधान है। दोबारा ऐसा प्रयास करने पर उसे 10 वर्ष के कारावास या 10 लाख रूपए जुर्माना अथवा दोनों सजा का प्रावधान भी किया गया है।
- **क्रिप्टोग्राफी, प्राइवेसी और राष्ट्रीय सुरक्षा** :– इंटरनेट द्वारा लोगों को अपना दृष्टिकोण प्रकट करने और किसी पर टिप्पणी करने का विश्वव्यापी मंच प्राप्त हो गया है। लेकिन इसका अर्थ यह नहीं है कि किसी को अमर्यादित रूप से किया जाए या उसकी प्राइवेसी में दखलंदाजी की जाए। अगर कोई ऐसा करता है तो वह साइबर अपराधी कहलायेगा। क्रिप्टोग्राफी वास्तव में शब्दों का प्रयोग कर संदेश को इस प्रकार प्रसारित करना है कि मात्र प्रेषण एवं संदेश द्वारा ही उसे समझ सके। इस प्रकार न केवल व्यक्ति की निजी स्वतंत्रता बनी रहती है बल्कि दूसरों को भी इन कोडवर्ड की जानकारी प्राप्त नहीं होती। आधुनिक युग में इस प्रकार के कार्यो में भी कोडवर्ड की चोरी करने एवं उन संदेशो का गैरकानूनी ढंग से अनाधिकृत व्यक्तियों व कंपनियों तक पहुंचने से व्यावसायिक संगठनों को ही नहीं बल्कि देश की सुरक्षा एजेंसियों के गुप्त कार्यो का पता दुश्मनों को चल जाता है जिस से राष्ट्रीय सुरक्षा खतरे में पड़ जाती हैं।

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

2) मूल शब्द (Keyword) :– भारत में बढ़ते साइबर अपराध एवं साइबर सुरक्षा का अध्ययन करना।

3) शोध अध्ययन प्रविधि :– वैज्ञानिक विश्लेषण और व्याख्या के लिए जिन वास्तविक तथ्यों की आवश्यकता होती है उन्हें एकत्रित करने के लिए अनुसंधानकर्ता द्वारा जिस विधि या तरीके को अपनाया जाता है उसे शोध प्रविधि कहते हैं। इस प्रकार यह स्पष्ट है कि प्रविधि वास्तव में वह साधन है जिनके माध्यम से अनुसंधान के लिए आवष्यक वास्तविक, तथ्यों सूचनाओं तथा आँकड़ो का संकलन किया जाता हैं।

प्रस्तुत अध्ययन में भारत सरकार के राष्ट्रीय अपराध रिकार्ड ब्यूरो के 2022 में प्रकाशित ''भारत में अपराध 2021'' रिपोर्ट को मुख्य स्त्रोत के रूप में शामिल किया है। प्रस्तुत शोध द्वितीयक आंकड़ों पर आधारित हैं।

4) अध्ययन के उद्देश्य :–

- भारत में हो रहे साइबर अपराध कि दर का अध्ययन करना।
- भारत में हो रहे साइबर अपराधों कि प्रकृति का अध्ययन करना।
- साइबर अपराध में शामिल हो रहे महिला–पुरूषों कि अपराध करने कि प्रवृत्ति का अध्ययन करना।

5) साहित्य की समीक्षा :– वृजेश और चौहान (2012) : लेखकों ने अपने पेपर में एक शोध किया ट्राइसिटी में साइबर क्राइम के प्रति जागरूकता और खुलासा कि जागरूकता उचित देकर बढ़ाई जा सकती है। साइबर अपराध के लिए महत्व जो एक हो सकता है, को कम करने या रोकने के लिए कुशल उपकरण साइबर अपराध। उन्होंने यह भी निष्कर्ष निकाला कि यह बना हुआ है। नेट उपयोगकर्ताओं के साथ–साथ उनकी भी जिम्मेदारी सरकार एक सुरक्षित, सुनिश्चित और सुनिश्चित करने के लिए भरोसेमंद कम्प्यूटिंग वातावरण।

मेहता और सिंह (2013) : लेखक ने भारतीय समाज में साइबर कानूनों के बारे में जागरूकता का अध्ययन करने के लिए एक सर्वेक्षण किया। उन्होंने पाया कि इंटरनेट सेवाओं के पुरूष और महिला उपयोगकर्ताओं के जागरूकता स्तर के बीच महत्वपूर्ण अंतर है। महिला

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

उपयोगकर्ताओं के जागरूकता स्तर के बीच महत्वपूर्ण अंतर है। महिला उपयोगकर्ताओं की तुलना में पुरूष नेटिजन्स साइबर कानूनों के बारे में अधिक जागरूक हैं।

अग्रवाल (2015) : लेखिका ने अपने पेपर में साइबर अपराध के प्रकार और उससे निपटने के लिए बनाए गए साइबर कानूनों पर चर्चा की। उनका उद्देश्य यह विश्लेषण करना था कि क्या इंटरनेट उपयोगकर्ता साइबर अपराधों के प्रति जागरूक हैं। उन्होंने इस बात पर भी जोर दिया कि साइबर अपराधों और साइबर कानूनों के बारे में जागरूक रहना सभी इंटरनेट उपयोगकर्ताओं का कर्त्तव्य है।

हसन (2015) : मलेशिया में साइबर अपराध जागरूकता का विश्लेषण करने के लिए एक सर्वेक्षण किया गया और पाया कि पुरूष छात्रों की तुलना में महिला छात्र साइबर अपराध के बारे में अधिक जागरूक हैं।

अर्चना चनुवाई नरहरि और वृजेश शाह (2016) : इसमें लेखक ने यह विश्लेषण करने के लिए 100 उत्तरदाताओं पर एक सर्वेक्षण किया कि क्या नेटिजन्स वास्तव में साइबर अपराधों के बारे में जानते है। उन्होंने पाया कि उत्तरदाता साइबर अपराधों, साइबर सुरक्षा के बारे में कुछ हद तक जागरूक हैं, लेकिन अभी भी उनमें जागरूकता बढ़ाने की जरूरत है। साथ ही उन्होंने एक वैचारिक मॉडल का सुझाव दिया जिसमें बताया गया कि साइबर अपराधों के संबंध में इंटरनेट उपयोगकर्ताओं के बीच जागरूकता कार्यक्रमों को कैसे बनाए रखा जाए और कैसे लागू किया जाए।

6) भारत में साइबर अपराध :– भारत में 'साइबर अपराध' शब्द का प्रयोग कम्प्यूटर या कम्प्यूटर नेटवर्क से जुड़ी आपराधिक गतिविधियों का वर्णन करने के लिए किया जाता है। इसके अंतर्गत कम्प्यूटर से संबंधित अवैध गतिविधियों की एक विस्तृत श्रंखला शामिल है, जैसे इलेक्ट्रॉनिक हैकिंग, सेवा क्षेत्र को बाधित करना, फिशिंग, क्रेडिट कार्ड धोखाधड़ी, बैंक डकैती, अवैध डाउनलोडिंग, चाइल्ड पोर्नोग्राफी, घोटाले, साइबर आतंकवाद और हानिकारक वायरस एवं स्पैम का निर्माण या वितरण आदि।

साइबर अपराध के अंतर्गत व्यक्तियों, संगठनों या यहाँ तक कि सरकारों को भी निशाना बनाया जाता है। साइबर अपराधों को मुख्यतः तीन श्रेणियों में विभाजित किया जा सकता हैः

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

- व्यक्तियों के विरूद्ध अपराध (जैसे यौन, नस्लीय या धार्मिक उद्देश्यों पर आधारित साइबर उत्पीड़न)
- संपत्ति के विरूद्ध अपराध (जैसे दूसरों के कम्प्यूटर डेटा को नष्ट करना, हानिकारक प्रोग्राम का प्रसार करना या कम्प्यूटर जानकारी तक अनाधिकृत पहुँच
- सरकार के विरूद्ध अपराध, जिसे साइबर– आतंकवाद के नाम से जाना जाता हैं।

भारत में इन साइबर अपराधों को रोकने के लिए विभिन्न हितधारकों को शामिल करते हुए एक बहु–आयामी दृष्टिकोण की आवश्यकता है।

सार्वजनिक जागरूकता :– जनसामान्य, व्यवसायों और संगठनों को साइबर सुरक्षा, खतरों तथा खतरों से निपटने के लिए विशिष्ट पद्धतियों एवं तकनीको के विषय में शिक्षित करना चाहिए। सुरक्षित इंटरनेट के उपयोग को बढ़ावा देने और सामान्य साइबर खतरों के बारे में जागरूकता बढ़ाने के लिए जागरूकता अभियान, कार्यशालाएं और प्रशिक्षण–सत्र आयोजित करना चाहिए।

साइबर सुरक्षा कानूनों को सशक्त करना :– उभरते साइबर खतरों को प्रभावी ढंग से संबोधित करने के लिए साइबर सुरक्षा कानूनों और विनियमों को लगातार अद्यतन और मजबूत करना चाहिए। इसके साथ ही यह सुनिश्चित करना चाहिए कि इंटरनेट अपराधों को गंभीर अपराध माना जाए और अपराधियों के लिए कठोर दंड का प्रावधान हों।

क्षमता–निर्माण :– विशेष प्रशिक्षण और संसाधन प्रदान कर, कानून प्रवर्तन एजेंसियों और साइबर सुरक्षा पेशेवरों की क्षमताओं में वृद्धि करनी चाहिए। साइबर अपराधों की जांच करने और घटनाओं पर तुरंत प्रतिक्रिया देने के लिए एक कुशल कार्यबल को गठित करना चाहिए।

साइबर सुरक्षा अवसंरचना :– संवेदनशील डेटा और प्रणाली को साइबर हमलों से बचाने के लिए वित्त, स्वास्थ्य सेवाओं जैसे महत्वपूर्ण क्षेत्रों के लिए सरकार को मजबूत साइबर सुरक्षा अवसंरचना में निवेश करना चाहिए।

सार्वजनिक–निजी भागीदारी :– साइबर हमलों की खुफिया जानकारी और उपयोगी तकनीकों को साझा करने के लिए सरकारी एजेंसियों, निजी व्यवसायों और साइबर सुरक्षा विशेषज्ञों के बीच सहयोग को बढ़ावा देना। सार्वजनिक–निजी भागीदारी साइबर हमलों को अधिक प्रभावी ढंग से पहचानने और प्रतिक्रिया देने में सहायता कर सकती है।

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

अंतर्राष्ट्रीय सहयोग :– सीमा–पार साइबर अपराधों से निपटने के लिए अंतर्राष्ट्रीय एजेंसियों और कानून प्रवर्तन के साथ सहयोग स्थापित करना। साइबर अपराधी प्रायः विभिन्न देशों में विभिन्न गतिविधियों में सलिंप्त होते हैं, तथा उन्हें ट्रैक करने और पकड़ने के लिए अंतर्राष्ट्रीय सहयोग आवश्यक हैं।

उत्तरदायी प्रकटीकरण को प्रोत्साहित करना : एथिकल हैकर्स और साइबर सुरक्षा शोधकर्ताओं को साइबर कमजोरियों के विषय में रिपोर्ट करने के लिए प्रोत्साहित करना चाहिए। ऐसी नीतियां को लागू करना चाहिए, जो प्रणाली और नेटवर्क में सुरक्षा खामियों की रिपोर्ट करने वालों को सुरक्षा प्रदान करें।

साइबर स्वच्छता :– अच्छी साइबर स्वच्छता तकनीकों को बढ़ावा देना, जैसे नियमित रूप से सॉफ्टवेयर अपडेट करना, मजबूत पासवर्ड का प्रयोग करना, दो–कारक प्रमाणीकरण सक्षम करना और वाई–फाई नेटवर्क को सुरक्षित करना। सुरक्षित कोडिंग तकनीकों को प्रोत्साहित करना, एप्लिकेशन और सॉफ्टवेयर में कमजोरियों को कम करने के लिए सॉफ्टवेयर डेवलपर्स के बीच सुरक्षित कोडिंग तकनीकों को बढ़ावा देना चाहिए।

प्रतिक्रिया एवं रिपोर्टिंग :–साइबर घटनाओं को रिपोर्टिंग के लिए एक सुव्यवस्थित तंत्र स्थापित करना और कानून प्रवर्तन अधिकारियों को साइबर अपराधों की त्वरित रिपोर्टिंग को प्रोत्साहित करना चाहिए।

मोबाइल सुरक्षा पर फोकस करना :–मोबाइल उपकरणों के बढ़ते प्रयोग को देखते हुए, उपयोगकर्ताओं को मोबाइल–आधारित साइबर खतरों से सुरक्षित रखने के लिए मोबाइल सुरक्षा पर ध्यान केंद्रित करना चाहिए। सतत् निगरानी और विश्लेषण, संभावित हमलों की पहचान करना और निवारक उपाय करने के लिए साइबर खतरों की सक्रिय निगरानी और विश्लेषण करना चाहिए।

7) निष्कर्ष :– इंटरनेट का उपयोग करने वाले लोगों की संख्या हर दिन बढ़ती जा रही है। दूसरी ओर साइबरस्पेस में अपराध भी तेजी से बढ़ रहे हैं। साइबर कमजोरियों को संबोधित करने के लिए सरकार, व्यवसायों, शैक्षणिक संस्थानों और व्यक्तियों सहित विभिन्न हितधारकों को ठोस प्रयास करने की आवश्यकता हैं। भारत में अपराधों से प्रभावी ढंग से निपटने के लिए साइबर सुरक्षा बुनियादी ढांचे को मजबूत करना, जागरूकता बढ़ाना, प्रभावी

ISSN PRINT 2319 1775 Online 2320 7876

 UGC CARE Listed (Group -I) Journal Volume 12,S Iss 1, 2023

साइबर सुरक्षा उपायों को लागू करना और सार्वजनिक और निजी क्षेत्रों के बीच सहयोग को बढ़ावा देना आवश्यक है।

इन रणनीतियों को लागू करके तथा एक सक्रिय और सहयोगात्मक दृष्टिकोण को अपनाकर भारत ऑनलाइन अपराधों को काफी हद तक कम कर सकता है और अपने नागरिकों एवं व्यवसायों के लिए एक सुरक्षित डिजिटल वातावरण बना सकता हैं।

8) सन्दर्भ सूची :–

1) जमील डी. और खान एम. एन. ए. (2011), यूरोपीय संघ के देशों की तुलना में भारत में डेटा संरक्षण अधिनियम, इलेक्ट्रिकल और कम्प्यूटर विज्ञान के अंतर्राष्ट्रीय जर्नल।

2) जैन, रोहित अरविंद (2018) ''साइबर अपराध और कानून, एविंसपब प्रकाशन।

3) चंदर, हरीश, ''साइबर कानून और आईटी संरक्षण।

4) डॉ. अग्रवाल, जी. के., ''समाजशास्त्र'' एसबीपीडी पब्लिशिंग हाउस।

5) हलदर, डी. और जयशंकर, के. (2011) साइबर अपराध और महिलाओं का शिकार : कानून, अधिकार और विनियम–हर्शे, पीए, यूएसए : आईजीआई ग्लोबल। आईएसबीएन 978–1–60960–830–9

6) मूर, आर. (2005) ''साइबर क्राइम : इन्वेस्टिगेटिंग हाई–टेक्नोलॉजी कम्प्यूटर क्राइम'' क्लवलैंड, मिसिसिपि : एंडरसन पब्लिशिंग।

7) अर्चना चनुवाई नरहरि और वृजेश शाह (2016) साइबर अपराध और सुरक्षा – आनंद के युवा नेटिजन्स के बीच जागरूकता पर एक अध्ययन। इंटरनेशनल जर्नल ऑफ एडवांस रिसर्च एंड इनोवेटिव आइडियाज शिक्षा, खण्ड–2, अंक–6

8) अवैस, एम. अब्दुल्ला और अन्य (2014) सिंध विश्वविद्यालय, जमशारो के छात्रों के बीच साइबर उत्पीड़न के बारे में जागरूकता। इंटरनेशनल जर्नल ऑफ एशियन सोशल साइंस, वॉल्यूम 4 (5), 632–641

9) हसन (2015), साइबर अपराध के प्रति युवा इंटरनेट उपयोगकर्ताओं की धारणा और जागरूकता : मलेशिया से साक्ष्य। जर्नल ऑफ सोशल साइंसेज, वॉल्यूम 11(4), 395–404