Naveen Shodh Sansar (An International Refereed / Peer Review Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 7.671
January to March 2024, E-Journal, Vol. I, Issue XLV

साइबर अपराध और सोशल मीडिया की भूमिका

डॉ. संगीता कुंभारे*

* सहायक प्राध्यापक (वाणिज्य) पंडित दीनदयाल उपाध्याय शासकीय कला एवं वाणिज्य महाविद्यालय, सागर (म.प्र.) भारत

शोध सारांश – साइबर अपराध एक ऐसा अपराध है जिसमें कंप्यूटर नेटवर्क और डिवाइस,नेटवर्किंग शामिल है कंप्यूटर का उपयोग अपराध करने के लिए किया जा सकता है और अक्सर लक्ष्य होते हैं साइबर अपराध किसी भी व्यक्ति या देश की सुरक्षा और वित्तीय स्वास्थ्य के लिए खतरा है।

डिजिटल वर्ल्ड में सुविधाओं के साथ–साथ साइबर क्राइम और जालसाजी के केस भी बढ़ रहे हैं एक रिपोर्ट के अनुसार साल 2021 में पिछले साल के मुकाबले साइबर क्राइम में 5 फीसदी की वृद्धि देखने को मिली है। साल 2021 में साइबर क्राइम 52,974 अपराध दर्ज किए गए हैं 2020 में अपराध के 50,035 मामले दर्ज किए गए थे। राष्ट्रीय अपराध रिकार्ड ब्यूरो NCRB की रिपोर्ट के अनुसार– –साइबर क्राइम के अधिकतर मामले उत्तर प्रदेश, तेलंगाना, कर्नाटक, असम और महाराष्ट्र में देखने को मिले हैं जबकि दिल्ली में साइबर अपराध के केवल 1.7 फीसदी देखे गए हैं।

जिनमें 2020 के मुकाबले 2021 में साइबर क्राइम के 5% मामले बड़े हैं साइबर क्राइम की घटनाओं की औसत दर 3.5 फीसदी (एक लाख आबादी) पर देखी गई है जबकि केवल एक तिहाई मामले ही दर्ज किए गए हैं। धोखाधड़ी के ज्यादा मामले आंकड़ों के अनुसार साइबर क्राइम में ज्यादातर मामले धोखाधड़ी के करीब 32,230 मामले मिले हैं यानी कि साइबर अपराध के कुल मामलों में 60.8 फीसदी मामले धोखाधड़ी के सामने आ रहे हैं।

समाज में कंप्यूटर के बढ़ते प्रयोग के साथ साइबर अपराध एक प्रमुख मुद्दा बन गया है। प्रौद्योगिकी को प्रकृति ने मनुष्य को अपनी सभी जरूर के लिए इंटरनेट पर निर्भर बना दिया है। साइबर अपराध समाज में होने वाले किसी भी अन्य अपराध से अलग हैं। इस कारण यह है कि इसकी कोई भौगोलिक सीमा नहीं है और साइबर अपराधी अज्ञात हैं यह सरकार व्यवसाय से लेकर नागरिकों तक सभी हितधारकों को समान रूप से प्रभावित कर रहा है भारत में सूचना और संचार प्रौद्योगिकी खउढ बढ़ती उपयोग के साथ साइबर अपराध बढ़ रहा है।

इसलिए प्रस्तुत विषय अंतर्गत साइबर अपराध के संक्षिप्त परिचय विभिन्न प्रकारों संशोधनों का अध्ययन करने और भारत में हो रहे साइबर अपराध का विश्लेषण करने का प्रयास किया गया है इसके अलावा भारत में साइबर अपराध पर काबू पाने के लिए कुछ कदमों पर चर्चा की गई है हम जितनी तेजी से डिजिटल दुनिया की ओर बढ़ रहे हैं ठीक उतनी ही तेजी से साइबर अपराध की संख्या में वृद्धि हो रही है जिस गति से तकनीक ने उन्नति की है,डिजिटल दुनिया की ओर ठीक साइबर अपराध की संख्या में वृद्धि हो रही है तकनीक ने लास्ट लाइन उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बड़ी है एक ही जगह पर बैठकर इंटरनेट के जरिए मनुष्य की पहुंच विश्व के किसी भी व्यक्ति तक आसान हो गई है।

देश के हर कोने तक आसान हुई है आज के समय में हर वह चीज इसके विषय में इंसान सोच सकता है समझ सकता है उसे तक उसकी पहुंच इंटरनेट के माध्यम से हो सकती है जैसे कि सोशल नेटवर्किंग साइट ऑनलाइन स्टडी ऑनलाइन जॉब इत्यादि आज के समय में इंटरनेट का उपयोग हर क्षेत्र में किया जाता है इंटरनेट के विकास और इसके संबंध लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है।

इंटरनेट के विकास और इसके संबंध लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है।

शब्द कुंजी – सोशल नेटवर्किंग साइट, इलेक्ट्रॉनिक डिवाइस, इंटरनेट कम्युनिकेशन टेक्नोलॉजी, अपराध।

प्रस्तावना

साइबर अपराध क्या है?

साइबर अपराध विभिन्न रूपों में किए जाते हैं कुछ साल पहले इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता का अभाव था साइबर अपराधों के मामले में भारत भी उन देशों से पीछे नहीं है जहां साइबर अपराधों की घटनाओं की दर भी दिन प्रतिदिन बढ़ती जा रही है। साइबर अपराध के मामलों में एक साइबर अपराधी उपयोग उपयोगकर्ता को व्यक्तिगत जानकारी गोपनीय व्यावसायिक जानकारी सरकारी जानकारी या किसी डिवाइस को बंद करने के लिए कर सकता है। किसी उपकरण का उपयोगकर्ता को व्यक्तिगत जानकारी,उपरोक्त सूचनाओं को ऑनलाइन खरीदना या बेचना भी एक साइबर अपराध है इसमें कोई संशय नहीं है कि यह एक आपराधिक गतिविधि है। कंप्यूटर और इंटरनेट के उपयोग के द्वारा यह अंजाम दिया जाता है। साइबर अपराध के रूप में भी माना जाता है। यह एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिए कंप्यूटर नेटवर्किंग साइट या नेटवर्क का उपयोग उपकरण के रूप में किया जाता है जहां इनके जरिए अपराधों को अंजाम दिया जाता है वही इन्हें लक्ष्य बनाते हुए इनके विरुद्ध अपराध भी किया जाता है।ऐसे अपराध में साइबर जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड, डेबिट कार्ड, एटीएम कार्ड की धोखाधड़ी, कंप्यूटर से डाटा हैक करना, अवैध डाउनलोडिंग, वायरस प्रसार सहित गतिविधियां शामिल है।

सॉफ्टवेयर चोरी भी साइबर अपराध की श्रेणी में आता है यह जरूरी नहीं की साइबर अपराध ऑनलाइन पोर्टल के माध्यम से ही किया जाए।

1. कंप्यूटर को हैक कर जानकारी प्राप्त करना।
2. कंप्यूटर को एक हथियार के रूप में प्रयोग करना साइबर आतंक, धोखाधड़ी, पोर्नोग्राफी आदि।

साइबर अपराध की श्रेणियां – साइबर अपराध के अंतर्गत प्रमुख श्रेणियां आती हैं जिनमें व्यक्ति विशेष संपत्ति और सरकार के विरुद्ध अपराध शामिल हैं।

व्यक्ति विशेष के विरूद्ध साइबर अपराध – ऐसे अपराध यद्यपि ऑनलाइन होते हैं परंतु वे वास्तविक लोगों के जीवन को प्रभावित करते हैं इनमें से कुछ अपराधों में साइबर उत्पीड़न और साइबर स्टॉकिंग, चाइल्ड पॉर्नोग्राफी की विवरण की जानकारी और विभिन्न प्रकार के कार्ड जिनके द्वारा लेनदेन किया जाता है पहचान की चोरी और मानव तस्करी पहचान ऑनलाइन बदनाम किया जाना शामिल है साइबर अपराध की इस श्रेणी में किसी व्यक्ति या समूह के खिलाफ दुर्भावना पूर्ण या अवैध जानकारी को ऑनलाइन लॉक कर दिया जाता है।

संपत्ति विशेष के विरूद्ध साइबर अपराध – कुछ ऑनलाइन अपराध संपत्ति के विरुद्ध होते हैं जैसे कि कंप्यूटर या सरवर के खिलाफ या उसे जरिया बनाकर किए जाते हैं। इन अपराधों में हैकिंग, वायरस ट्रांसमिशन, साइबर कॉपीराइट उल्लंघन आदि शामिल है।

उदाहरण– कोई आपको एक वेबलिंक भेजें जिस पर क्लिक करने के पश्चात एक वेब पेज खुलेगा जहां आपसे बैंक खाता संबंधी एवं दस्तावेज संबंधी संपूर्ण जानकारी मांगी जा रही है और आप वह जानकारी देते हैं। आपके दस्तावेज एवं बैंक खाते के साथ छेड़छाड़ की जाएगी और यह संपत्ति के विरूद्ध साइबर हमला कहा जा सकता है।

सरकार विशेष के विरूद्ध साइबर अपराध – यह सबसे गंभीर साइबर अपराध माना जाता है सरकार के खिलाफ किए गए ऐसे अपराध को साइबर आतंक के रूप में भी जाना जाता है सरकारी साइबर अपराध में सरकारी वेबसाइट या सैन्य वेबसाइट को हैक किया जाना शामिल है एक साइबर अपराध किया जाता है तो इसे उसे राष्ट्र की संप्रभुता पर हमला माना जाता है।

यह अपराध आमतौर पर आतंकवादी या अन्य शत्रु देश की सरकारें करती हैं इस प्रकार के साइबर अपराध पर नियंत्रण के लिए प्रत्येक देश की सरकार द्वारा कठोर साइबर कानून बनाए गए हैं।

आपातकालीन स्थिति में या साइबर अपराधों के अलावा अन्य अपराधों की रिपोर्ट करने के लिए स्थानीय पुलिस से संपर्क करें एवं राष्ट्रीय पुलिस हेल्पलाइन नंबर 112 है। और साइबर अपराध हेल्पलाइन नंबर 130 है।

Year	IT Act		IPC	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
2014	7201	4246	3272	3224
2015	8045	5102	3422	2867
Total	24269	14552	8854	8289

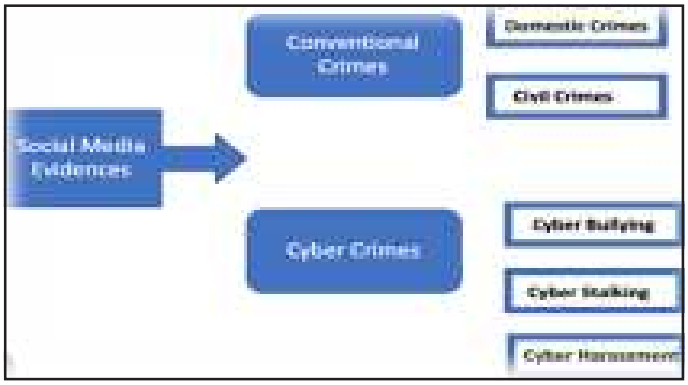
सोशल मीडिया की भूमिका – बड़े पैमाने पर सोशल नेटवर्किंग साइट का उपयोग करने वाली जनसंख्या साइबर अपराध की खतरों से अनजान हैं जिनमें सोशल नेटवर्किंग साइट के सर्वर अन्य देशों के कंट्रोल में है एवं वहां पर केंद्रित हैं जिससे यह डर रहता है कि कहीं यह देश लोगों की व्यक्तिगत जानकारी का दुरुपयोग ना करें।

लोगों को विभिन्न सोशल नेटवर्किंग साइट पर हैकर्स ऑनलाइन ठगी का शिकार बनाते हैं।

सुरक्षा एजेंसी द्वारा यह पता लगाया जाता है ऑनलाइन मुद्रा स्थानांतरित करने वाले विभिन्न एप के माध्यम से आतंकवाद दोनों और देश विरोधी तत्वों को फंडिंग की जाती है साइबर अपराधी विभिन्न ऑनलाइन गेम्स के माध्यम से बच्चों को अपराध करने के लिए प्रोत्साहित करते हैं।

सोशल मीडिया पर साइबर अपराध का तात्पर्य व्यक्तियों या समूह द्वारा दुर्भावना पूर्ण इरादे से की जाने वाली व्यापक अवैध गतिविधियों से है यह गतिविधियां व्यक्तियों के संगठनों या यहां तक की सरकारों को भी लक्षण कर सकती हैं, और इनमें ऑनलाइन धोखाधड़ी, उत्पीड़न और धोखे के विभिन्न रूप भी शामिल हैं।

अश्लील इलेक्ट्रॉनिक सामग्री प्रकाशित करने पर 5 साल की कैद और जुर्माना हो सकता है। 10 लाख जुर्माना भी राष्ट्रीय सुरक्षा को प्रभावित करने वाले साइबर अपराधों में आजीवन कारावास हो सकता है अन्य साइबर अपराधों के लिए 3 साल तक की कैद या जुर्माना या दोनों की कम सजा निर्धारित है।



साइबर अपराधों से निपटने की दिशा में सरकार की प्रयास–भारत सरकार द्वारा सूचना प्रौद्योगिकी अधिनियम 2000 पारित किया गया। जिनके प्रावधानों के साथ–साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिए पर्याप्त हैं।

अध्ययन एवं विश्लेषण– सूचना प्रौद्योगिकी अधिनियम 2000 की धाराएं

43,43A,66,66B,66C, 66D,66E,66F,67,67A,67B आदि हैकिंग और साइबर अपराधों से संबंधित हैं।

सरकार द्वारा राष्ट्रीय साइबर सुरक्षा नीति 2013 जारी की गई जिसके तहत सरकार ने अति संवेदनशील सूचनाओं के संरक्षण के लिए राष्ट्रीय अति संवेदनशील सूचना अवधारणा संरक्षण केंद्र का गठन किया गया NCIIPC: नेशनल क्रिटिकल इनफॉरमेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर। इसके अंतर्गत दो वर्ष से लेकर उम्र कैद तथा अर्थ दंड का भी प्रावधान है विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित से सरकार ने सूचना सुरक्षा शिक्षा और जागरूकता परियोजना आरंभ की है।

सरकार द्वारा कंप्यूटर इमरजेंसी रिस्पांस टीम की स्थापना की गई जो सुरक्षा के लिए राष्ट्रीय स्तर की मॉडल एजेंसी है।

भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्ताम कार्य प्रणाली अपनाने के लिए अमेरिका ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है।

इस योजना को संपूर्ण भारत में लागू किया गया है बेहतर तरीके से निपटने के लिए तथा 14C समन्वित और प्रभावी तरीके से लागू करने हेतु इस योजना के निम्नलिखित सात प्रमुख घटक हैं।

1. नेशनल साइबर क्राइम थ्रेट एनालिटिक्स यूनिट
2. नेशनल साइबर क्राईम रिर्पोटिंग पोर्टल
3. प्लेटफॉर्म फॉर जॉइंट साइबर क्राईम इन्वेस्टिगेशन टीम
4. नेशनल साइबर क्राइम फॉरेंसिक लेबोरेटरी इकोसिस्टम
5. नेशनल साइबर क्राइम ट्रेनिंग सेंटर
6. नेशनल साइबर रिसर्च एंड इन्नोवेशन सेंटर

बुडापोस्ट कन्वेंशन क्या है?

साइबर अपराध के संबंध में बुडापोस्ट कन्वेंशन सेंटर पर हस्ताक्षर करने के लिए गृह मंत्रालय द्वारा साइबर अपराध और डेटा सुरक्षा को बढ़ावा देने के लिए राष्ट्रीय सहयोग की आवश्यकता पर बोल दिया जा रहा है।

बुडापोस्ट कन्वेंशन साइबर क्राइम पर एक कन्वेंशन है जिसे साइबर अपराध पर बुडापोस्ट कन्वेंशन के नाम से जाना जाता है।

यह अपनी तरफ से पहले ऐसा अंतरराष्ट्रीय समझौता जिसके अंतर्गत राष्ट्रीय कानून को व्यवस्थित करके जांच पड़ताल की तकनीक में सुधार करने तथा इस संबंध में विश्व के अन्य देशों में सहयोग को बढ़ाने हेतु और कंप्यूटर अपराधों पर रोक लगाने संबंधी मांग की गई है।

शोध की परिकल्पना– वर्तमान में भारत की आबादी बहुत ज्यादा है नेटवर्किंग साइट का उपयोग करती है भारत में सोशल नेटवर्किंग साइट के उपयोग भी बड़े हैं इनमें जानकारी का अभाव है सोशल नेटवर्किंग साइट के सरवर विदेश में है जिससे भारत में साइबर अपराध घटित होने की स्थिति में इनकी जड़ तक पहुंच पाना कठिन होता है।

इस आलेख में साइबर अपराध प्रकार के और सरकार के द्वारा किए गए प्रावधानों पर विमर्श किया जाएगा इसके साथ ही साइबर अपराध में सोशल नेटवर्किंग साइट की भूमिका का भी मूल्यांकन किया जाएगा।

निष्कर्ष– भारत इंटरनेट का तीसरा सबसे बड़ा उपयोग करता है और हाल ही के वर्षों में साइबर अपराध कई गुना बढ़ गए हैं। साइबर सुरक्षा उपलब्ध कराने के लिए सरकार की ओर से कई कदम उठाए गए हैं कैशलेस अर्थव्यवस्था को अपनाने की दिशा में बढ़ाने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी अत: भारत को इस क्षेत्र में तीव्र गति से कार्य करना होगा वहीं दूसरी ओर सोशल मीडिया ने अभीव्यक्ति की स्वतंत्रता के अधिकार को नया आयाम दिया है। आज प्रत्येक व्यक्ति बिना किसी डर के सोशल मीडिया के माध्यम से अपने विचार रख सकता है और उसे हजारों लोगों तक पहुंचा सकता है परंतु सोशल मीडिया का सावधानीपूर्वक उपयोग ही हमें ऑनलाइन ठगी साइबर अपराध के गंभीर खतरों से बचा जा सकता है।

हम एक डिजिटल युग में रह रहे हैं और साइबर स्पेस किसी भी सीमाओं तक सीमित नहीं है बल्कि यह पूरी दुनिया को कवर करता है परिणाम स्वरुप साइबर क्राइम दिन प्रतिदिन बढ़ता ही जा रहा है। डिजिटल प्रौद्योगिकी के चल रहे विकास के कारण सबसे बड़ी चुनौती साइबर अपराध की गतिशील प्रकृति से संबंधित है।परिणाम स्वरुप साइबर अपराध के नए तरीके और तकनीक प्रचलन में आती है इसलिए साइबर क्राइम को भी उतना ही महत्व दिया जाना चाहिए। जितना कि हमारे समाज में हो रहे अन्य अपराध।

संदर्भ ग्रंथ सूची :–

1. दैनिक भास्कर समाचार पत्र
2. पत्रिका समाचारपत्र
3. अनिमेश शर्मा साइबर सुरक्षा मुद्दे वर्तमान भारतीय साइबर कानून और उठाए जाने वाले कम
4. अन्य वेबसाइट
5. https://www.drishtiias.com/
6. https://cybercrime.gov.in/
7. National Cyber Crime Reporting Portal

****