International Research Journal of Human Resource and Social Sciences
ISSN(O): (2349-4085) ISSN(P): (2394-4218)
Impact Factor 7.924 Volume 11, Issue 01, Jan 2024
Website- www.aarf.asia, **Email** : editoraarf@gmail.com

सायबर अपराध एवं सायबर कानून चुनौतियां और रोकथामः एक अध्ययन

डॉ.आर.एन. शर्मा,
विभागाध्यक्ष, समाज विज्ञान संकाय,
श्री सांई बाबा आदर्श महाविद्यालय, अम्बिकापुर
dr.ravindrasharma@yahoo.com

संक्षेपिका –

डिजिटल तकनीक के विस्तार के साथ ही साइबर अपराध का स्वरूप और दायरा भी व्यापक होता जा रहा है। यह शोध–पत्र साइबर अपराधों की प्रकृति, कारण, इसके सामाजिक व आर्थिक प्रभाव, भारत में लागू साइबर कानूनों की स्थिति, उनकी चुनौतियां और प्रभावी रोकथाम के उपायों का विश्लेषण करता है। अपराध की अवधारणा मानव समाज के उद्‌गम के साथ ही प्रारंभ हुयी है। सामान्य अर्थो में कोई भी ऐसा कृत्य जो विधि के विरूद्ध हो तथा जिसके लिये उचित दण्ड की व्यवस्था हो, अपराध कहलाता है। आदिम समाजों में हत्या, लूटपाट, डकैती, बलात्कार, युद्ध इत्यादि अपराध के रूप मे विद्यमान रहे हैं। मानव समाज के विकास के साथ अपराध की अवधारणा में भी परिवर्तन हुआ है, वर्तमान में पूर्व की भांति कोई दस्यु डाकू या बीहड़ में बैठकर अपराध करने वाली महज अपराधी नहीं है, बल्कि आज के अपराधी तकनीकी युग के जानकार हैं। वह अब बड़े कमरों में बैठकर कम्प्यूटर व इन्टरनेट के माध्यम से अपराध कर रहा है। किसी भी कम्प्यूटर या अन्य संचार माध्यम से किया जाने वाला अपराध सायबर अपराध कहलाता है।

प्रस्तावना –

सूचना और संचार प्रौद्योगिकी ने मानव जीवन को सरल और सुगम बनाया है, परंतु इसी तकनीकी विकास ने अपराध का नया माध्यम साइबर अपराध भी जन्म दिया है। साइबर अपराध ऐसे अपराध हैं, जिनमें कंप्यूटर, इंटरनेट या नेटवर्क का उपयोग कर गैरकानूनी गतिविधियां की जाती हैं। इनके कारण व्यक्तिगत जीवन, आर्थिक व्यवस्था, सामाजिक संरचना तथा राष्ट्रीय सुरक्षा तक प्रभावित होती है। सायबर शब्द का सर्वप्रथम उल्लेख विलियम गिब्सन की कृति 'न्यूरान एन्सर' में 1948 में मिलता है। विलियम ने इसमे सायबर स्पेस का उल्लेख किया था, जिसका अर्थ होता है छवियों के कम्प्यूटर द्वारा त्रिआयामी रेखाचित्र। यूरोपियन सायबर क्राइम टीटी काउंसिल के अनुसार 'सायबर क्राइम एक ऐसा अपराध है जो कि डेटा एवं कॉपीराइट के विरुद्ध की गयी अपराधिक गतिविधि है। इस अपराध के अर्न्तगत जालसाजी, अनाधिकृत प्रवेश, चाइल्ड पोर्नोग्राफ और सायबर स्टॉकिंग शामिल है। सायबर अपराध वह अपराध है जिसमे कम्प्यूटर इन्टरनेट नेटवर्क एवं हार्डवेयर तथा उससे सम्बंधित उपकरण, प्रिन्टर, स्कैनर इत्यादि का प्रयोग किया गया है। यह दुनिया के किसी भी व्यक्ति के द्वारा कहीं भी बैठकर अंजाम दिया जा सकता है। सायबर अपराध मुख्य रूप से समाज को कई प्रकार से प्रभावित करता है। किसी व्यक्ति के विरूद्ध, किसी संगठन के विरूद्ध ,सम्पूर्ण समाज के विरूद्ध, संपत्ति के विरूद्ध व सरकार के विरूद्ध आदि अनेक प्रकार के सायबर अपराध के प्रभाव हैं।

1. **सायबर अपराध** – पासवर्ड की चोरी, एकाउन्ट से निजी सम्पत्ति की चोरी , किसी व्यक्ति से सम्बन्धित अश्लील या आपत्तिजनक या गोपनीय जानकारी को प्रचारित करना, कम्प्यूटर वायरस द्वारा उसके दस्तावेजो को नष्ट करना, क्रेडिट कार्ड का अनाधिकृत उपयोग करना, गंदे ई–मेल करना आदि व्यक्ति के विरूद्व सायबर अपराध के स्वरूप हैं। संस्था या संगठन के विरूद्ध सायबर अपराध में हैकिंग या क्रैकिंग तथा आकड़ों की चोरी, आकड़ों को नष्ट करना अनाधिकृत सूचनादि प्राप्त करना या पायरेटेड सॉफ्टवेयर का वितरण एवं कानून का उल्लंघन करना शामिल है। इसी प्रकार सम्पूर्ण समाज के विरूद्ध सायबर अपराध के रूप में अश्लील एवं नग्न चित्रो को नेट पर प्रचारित करना, पोर्नोग्राफी, टैफिकिंग द्वारा दूषित वातावरण बनाना इत्यादि शामिल है। प्रसिद्ध व्यक्ति, फिल्मी अभिनेत्रियों के अश्लील चित्र बनाकर नेट पर प्रकाशित करना भी इसी अपराध की श्रेणी मे आता है। इसका प्रभाव सम्पूर्ण समाज में पड़ता है। धोखाधडी, बौद्विक संपत्ति के विरूद्व ,कापीराइट का उल्लंघन आदि व्यक्ति के विरूद्ध तथा सायबर आतंकवाद,शासकीय वेबसाइट को हैक करना,आंकडे चुराना,आदि सरकार के विरूद्ध किये जाने वाले सायबर अपराध के उदाहरण हैं।

2. **सायबर अपराधी** – आज के इस कम्प्यूटर युग में दुनिया के कोने–कोने में कम्प्यूटर, इंटरनेट व सायबर अपराधी विद्यमान हैं। सायबर अपराधी के रूप में किशोर ,संगठित हैकर्स एवं क्रैकर्स, व्यावसायिक हैकर्स, कंपनी के कार्य करने वाले असंतुष्ट कर्मचारी, विभिन्न खूफिया एजेन्सी के जासूस, पॉलिटिकल हैक्टिविस्ट, पूर्व प्रेमी तथा तलाकशुदा, आतंकवादी संगठन कोई भी हो सकता है। फेडरल ब्यूरो ऑफ इन्वेस्टीगेशन के आकड़ों के मतानुसार 46 प्रतिशत कंपनी में नियुक्त कर्मचारी चोरी कर अन्य कंपनी को सूचनाओं का आदान–प्रदान करते है। प्रत्येक 10 ई–मेल मे से 9 ई–मेल जंक मेल है। बाजार में उपलब्ध सॉफ्टवेयर में से 58 प्रतिशत सॉफ्टवेयर पाइरेटेड है। इन्टरनेट पर कार्य करने वाले 37 प्रतिशत लोग अश्लील साइट्स देखते है। 42 प्रतिशत लोग इन्टरनेट पर अश्लील वार्तालाप करते है। वायरल आक्रमण प्रतिवर्ष 50 प्रतिशत की दर से बढ़ रहा है। औद्योगिक क्षेत्र में सोर्स कार्ड की चोरी 37 प्रतिशत, व्यावसायिक प्रयोजनी चोरी 28 प्रतिशत, क्रेडिड कार्ड सूचना चोरी 29 प्रतिशत तक पायी गयी है ।

सायबर अपराध– प्रकृति– वर्तमान में इंटरनेट प्रयोक्ताओं के बढ़ने के साथ–साथ सायबर अपराध भी निरंतर बढ़ रहे हैं। आज जहॉ सोशल नेटवर्किंग वेबसाइट्स सामाजिक नेटवर्क व संपर्क का अद्भूत मिसाल प्रस्तुत कर रही है वहीं इनसे संबंधित सायबर अपराध भी पनप रहे हैं जिनमें निजता का उल्लंघन, पहचान की चोरी, व्यक्तिगत आंकड़े चुराना, प्रोफाइल पर गंदे संदेश या तस्वीर भेजना आदि शामिल है। इसके साथ ही समाज में अश्लीलता फैलाना, परंपराओं व संस्कृतियों या धार्मिक आस्थाओं के साथ छेड़छाड़ करना आदि समाज में इसके दुष्प्रभाव के रूप में प्रकट हो रहे हैं। बच्चों व महिलाओं का अश्लील प्रस्तुतीकरण उनके समाज में सम्मान व सुरक्षा को घटाता है। आज इंटरनेट पर विवाह संपन्न कराने के नाम पर अनेक धोखाधड़ी के प्रकरण सामने आ रहे हैं। सरकार व शासन के खिलाफ आतंकी गतिविधियॉ करने हेतु इंटरनेट का प्रयोग करना व ईमेल, ई–बैंकिग, ई–कॉलिंग, आदि के द्वारा सायबर आतंकवाद को बढ़ावा देने संबंधी पहलू भी उजागर हो रहे हैं।

भारत में सायबर अपराध की प्रवृत्ति – राष्ट्रीय क्राइम रिकार्ड ब्यूरो द्वारा 2010 में जारी भारत में अपराधष नामक रिर्पोट में सायबर अपराध का विश्लेषण प्रस्तुत किया गया है तथा नवीन उभरती प्रवृतियों पर प्रकाश डाला गया है। राष्ट्रीय क्राइम रिकार्ड ब्यूरो के अनुसार 2010 में 1322 अपराध 2009 में 696 अपराध की तुलना में सायबर अपराध में 90 प्रतिशत की वृद्वि हुई है। इसमें बताया गया है कि सबसे अधिक संख्या में सायबर अपराध कम्प्यूटर सूचनाओं की हानि या नुकसान से संबंधित दर्ज किये गये हैं। ज्यादातर अपराधों के उद्देश्य अवैध रूप से धोखाधड़ी करने या जालसाजी से संबंधित हैं।

नार्टन सायबर अपराध रिपोर्ट 2011 में भारत में सायबर अपराध से होने वाले कुल नुकसान को लगभग 34200 करोड़ रूपये आंका गया है। साथ ही इस रिपोर्ट में भारत में इंटरनेट का प्रयोग करने वाले 5 में से 4 व्यक्ति को सायबर अपराध का शिकार बताया गया है।

एक अन्य रिपोर्ट के अनुसार 2010 से 2011 के मध्य 12 सरकारी वेबसाइटों को सायबर अपराधियों ने अपना शिकार बनाया है। जिसमें एनआईसी की वेबसाइट हैकिंग का उदाहरण प्रमुख है।

भारत में सायबर अपराध के कारण–

भारत में इंटरनेट प्रयोक्ताओ की संख्या तथा इसका दुरूप्रयोग करने वालों व इसे माध्यम बना कर अपराध को अन्जाम देने वालो की संख्या निरंतर बढती जा रही है। सायबर अपराध को अंजाम देने वालो में उस कम्प्यूटर शिक्षित वर्ग का स्थान है जो अपने ज्ञान का दूरूप्रयोग करते हुए दूसरों को नुकसान पहुचाते हैं। सायबर अपराध को कारित करने के पीछे अनेक कारणो की पहचान की जा सकती है जिसमें कुछ प्रमुख कारण इस प्रकार है –

(1) आर्थिक लाभ के लिए– इसके अन्तर्गत इंटरनेट के जरिये, ईमेल के माध्यम से, क्रेडिट कार्ड, डेबिट कार्ड का पास वर्ड हैक करके, बैंक एकांउट हैक करके, पासवर्ड हैक करके अपराधी लाभ उठाता है। इसमे दो युवको के द्वारा भेल के 3500 शेयर हैक करके बाजार मे बेचकर आर्थिक लाभ अर्जित करने का उदाहरण प्रमुख है जिन पर कंपनी के द्वारा बाद में अपराध दर्ज कराया गया है ।

(2) बदला लेने के लिए– स्कुल कालेज के साथी या सहकर्मी या प्यार में असफल व्यक्तियो के द्वारा अपनी शत्रुता को अन्जाम देने अथवा भयभीत करने के लिये, धमकी भरे इमेल भेज कर, व्यक्तिगत या अश्लील चित्रो या वीडियो को अपलोड कर बदला लेने की नीयत से अपराध कारित किया जाता है।

(3) कुंठित यौन भावनाओ को अन्जाम देने के लिये– युवा वर्ग के द्वारा यौन कुंठाओ की पूर्ति के लिये अश्लील बेवसाइट सर्च किया जाता है तथा रिले चैट/वीडियो चैट के माध्यम से अवैधानिक एवं अश्लील घटनाओ को अन्जाम दिया जाता है। एमएमएस स्कैण्डल्स भी इसी श्रेणी के अपराध है।

(4) राष्ट्र के विरूद्व – वर्तमान मे सायबर आंतकवाद के रूप मे इंटरनेट का उपयोग राष्ट्र के विरूद्व आतंक फैलाने में किया जा रहा है। इसमे देश के प्रतिष्ठित पद पर कार्यरत राष्ट्र प्रमुखो को धमकाना, बम धमाके के लिये इमेल का प्रयोग करना, ई–बैकिंग का उपयोग कर प्रतिबंधित या आतंकी संगठनों को वित्तीय मदद करना आदि अपराध कारित किये जा रहे है। इसमें राष्ट्र की प्रमुख वेबसाइटो को हैंक कर सुचनाओ की चोरी करने का प्रयास भी शामिल है।

(5) अनुचित लाभ के लिये – लायसेंसी साफ्टेवयर का उपयोग न करना, बौद्विक सम्पत्ति व कापीराइट संबंधी विधिक प्रावधानों का उल्लंघन करने वाले सायबर अपराध संगठनों व संस्थाओं को नुकसान पहुंचाकर अनुचित लाभ कमाने के उद्देश्य से किये जाते हैं।

(6) असुरक्षित इंटरनेट पयोग के कारण – इंटरनेट प्रयोक्ताओ द्वारा असुरक्षित तरीके से इंटरनेट का प्रयोग करना, अपने ईमेल पासवर्ड को संभाल कर न रखना, लालच में आकर इंनटरनेट पर अंजान व्यक्ति को अपनी व्यक्तिगत सूचनाये प्रदान करना, वाईफाई को पासवर्ड से सुरक्षित न करना, एंटीवायरस या पाप अप ब्लाकर का उचित उपयोग न करना आदि अन्य कारण सायबर अपराध को बढ़ावा देते है।

भारत में सायबर अपाराध पर नियंत्रण हेतु विद्यमान कानुन

(1) सूचना प्रौधौगिकी अधिनियम 2000 व 2008 –

प्रमुख प्रावधान :–

1. धारा 65 – कम्प्यूटर सोर्स विभाग में अनाधिकृत परिवर्तन
2. धारा 66 – हैकिंग के जरिये कम्प्यूटर की उपयोगिता के रूप में हानि/नष्ट करना ।
3. धारा 66(2)– हैकिंग
4. धारा 67 – अष्लील साहित्य का प्रकाषन और इलेक्ट्रानिक रूप से सम्प्रेषण ।
5. धारा 70 – अनाधिकृत पहुंच।
6. धारा 71 – झुठे प्रमाण पत्रो का प्रकाषन ।
7. धरा 72 – विष्वास /निजता/विच्छेद का उल्लंधन
8. धारा 73/74 – डिजिटल हस्ताक्षरों की जालसाजी ।

(2) भारतीय दंड विधान 1860 के अंतर्गत प्रावधान –

1. साक्ष्यो से संबंधित सायबर अपराध – धारा 193, 204 ,477
2. धोखाधडी से संबंधित सायबर अपराध – धारा 463, 465, 466 ,471, 474, 476, 477–अ
3. आपराधिक न्यासभंग से संबंधित सायबर अपराध – धारा 405 .406, 408, 409
4. कम्प्यूटर से छेडछाड से संबधित सायबर अपराध – धारा 489
5. मुद्रा/स्टाम्प से संबंधित सायबर अपराध –482,483,484,488,489,489–स

(3) भारतीय साक्ष्य अधिनियम 1872 के अंतर्गत प्रावधान –

धारा 17, 22–अ, 34, 39 ,47–अ, 65–अ, 65–ब, 67–अ ,73–अ,81–अ,65–अ,ब,स, ,88–अ आदि प्रमुख हैं।

पुलिस की भूमिका

सायबर अपराधो के घटित होने के बाद इसकी विवेचना पुलिस के द्वारा की जाती है। सायबर अपराध का शिकार होने पर पीडित व्यक्ति के द्वारा कम्प्यूटर सिस्टम से छेडछाड नही करना चाहिये व तत्काल पुलिस को सूचना देनी चाहिये तथा सायबर अपराधी की पहचान कर सूचना प्रौधौगिकी अधिनियम 2000 के तहत अपराध पजीबंद्व कराना चाहिये तथा साक्ष्य संकलन में पुलिस की सहायता करनी चाहिए। वर्तमान में भारत में दर्ज किये जाने वाले सायबर अपराधो की संख्या वास्तविक रूप से घटित होने वाले सायबर अपराधो से काफी कम है। सायबर अपराधो की दर्ज संख्या कम होने के दो प्रमुख कारण हैं। प्रथम पीडित व्यक्ति के द्वारा अनेक अवसरो पर नजरअंदाज कर दिया जाता है या वह पर्याप्त जागरूक नही होता, द्वितीय पुलिस के द्वारा सूचना तकनीक अधि. के तहत अपराध दर्ज करने से बचने का प्रयास किया जाता है तथा भा.द.वि. के

तहत ही दर्ज कर लिया जाता है। सायबर अपराध के संदर्भ में पुलिस की शिथिलता के अनेक कारक है जिनमे कार्यरत् पुलिस कर्मियो में कम्प्यूटर व अंग्रेजी साक्षरता का प्रतिषत अत्यंत निम्न होना, सायबर अपराध की जांच हेतु प्रशिक्षण का अभाव, आई.टी. एक्ट 2000 के संदर्भ में जानकारी का अभाव सायबर पुलिस थानो का अभाव, पुलिस थाानो में कम्प्यूटर की अपर्याप्त उपलब्धता या अनुपलब्धता, सायबर अपराध की विवेचना तकनीक व प्रयोग होने वाले उपकरणो की जानकारी न होना आदि प्रमुख हैं।

सायबर अपराध के अन्वेषण/विवेचना में पुलिस की भूमिका

सायबर अपराध की विवेचना में पुलिस द्वारा अपनाये जाने वाले प्रक्रिया का संक्षिप्त विवरण इस प्रकार हैः–

(1) सायबर अन्वेषण/विवेचना – कम्प्यूटर या सायबर अपराध विवेचना वह प्रक्रिया है जिसमें डिजीटल साक्ष्यो का पहचान,संरक्षण,विष्लेषण इस प्रकार से किया जाता है कि न्यायलयो में वे विधिक रूप से स्वीकार्य हों।साक्ष्य के इस प्रक्रिया या नियमों के अतंर्गत स्वीकार्यता (न्यायालय में), प्रमाणिकता (घटना के संबंध में),पूर्णता, विष्वासनीयता आदि शामिल होते है।सायबर अपराधो की विवेचना करने वाले प्रत्येक अधि./कर्मचारी (पुलिसकर्मी) को इलेक्ट्रानिक साक्ष्यो की नाजुक प्रकृति व उसके संग्रहण व संरक्षण से संबंधित सिद्धांतो व प्रक्रियाओ को समझना आवष्यक है । सायबर अपराध अन्वेषण प्रक्रिया के अनेक चरणो में 5 प्रमुख चरण हैंः–

1. **पहचान व मान्यता –प्रलेखन** – साक्ष्य के रूप में घटनास्थल पर विद्यमान विभिन्न कम्प्यूटर सिस्टम, बाह्य उपकरण आदि की पहचान तथा घटनास्थल पर उपस्थित व्यक्तियो व संचार के माध्यमो की पहचान ताकि प्रकरण में महत्वपूर्ण भूमिका रखने वाले उपकरणो को पहचाना जा सके ।
2. **संग्रहण – प्रलेखन** – संग्रहण चरण इलेक्ट्रानिक साक्ष्यो की मान्यता (पहचान) , संग्रह तथा दस्तावेजीकारण हेतु खोज सम्मिलित करता है। संग्रहण चरण उन वास्तविक समय के तथा संग्रहित जानकारियो को समाहित करता है जो कि घटना स्थल पर लापरवाही बरतने पर नष्ट हो सकतें है।
3. **परीक्षण विश्लेषण – प्रलेखन** – परीक्षण की प्रक्रिया साक्ष्य को दृष्य बनाने तथा उसके उत्पत्ति व महत्व को जानने में सहायता करता है।
4. **विश्लेषण – प्रलेखन** – विष्लेषण की प्रक्रिया में परीक्षण से प्राप्त तथ्यो का, जांच संबंधी मामले में महत्व व मूल्य का जांच किया जाता है।
5. **संचार या रिपोर्टिंग – प्रलेखन**– रिपोर्टिंग चरण में संपूर्ण जांच/अन्वेषण प्रक्रिया का विवरण तथा बरामद प्रासंगिक डाटा को प्रस्तुत किया जाता है।

(2) सायबर अपराध अन्वेषण का कार्डिनल नियम :–

1. साक्ष्य को कभी लापरवाहीपूर्वक हैडंल न करें।
2. मषीन या विषय आपरेटिंग सिस्टम पर कभी भरोसा न करें।
3. कभी मूल साक्ष्य पर काम न करें,उसकी प्रति तैयार करें।
4. सभी तथ्यों का दस्तावेजीकरण (प्रलेखन) करें।

❖ **विवेचना प्रारंम्भ करने से पूर्व निम्न तथ्यो का निर्धारण आवश्यक रूप से किया जाना चाहिये –**

1. वह कम्प्यूटर जिसे साक्ष्य के रूप मे जब्त किया जाना है उसकी संबंधित प्रकरण में क्या भूमिका है।
2. वह कम्प्यूटर संदेही का है अथवा पीडित का है।
3. क्या वह कम्प्यूटर अपराध कारित करने के लिये मध्यस्थ उपकरण के रूप में प्रयोग किया गया है।
4. क्या साक्ष्य दिखाई दे रहे है ।
5. संदिग्ध /आरोपी का सुक्ष्म इंटरव्यू लिया जाना चाहिये ।

इलेक्ट्रानिक साक्ष्य

डिजीटल सबूत या इलेक्ट्रानिक साक्ष्य किसी भी प्रमाण के लिये संग्रहित या डिजीटल रूप में प्रेषित जानकारी है जिसे न्यायालय के समक्ष किसी पक्ष के विरूद्ध मुकदमें में उपयोग किया जाता है।

सायबर अपराध घटनास्थल में इलेक्ट्रानिक साक्ष्यो के संकलन/हैडंलिंग हेतु सामान्य निम्न चरणो /नियमो का पालन किया जाता हैः–

1. साक्ष्यो की पहचान व मान्यता
2. अपराध व अपराध स्थल का दस्तावेजीकरण
3. साक्ष्यो का संग्रहण व संरक्षण
4. साक्ष्यो की पैकिजिंग व परिवहन व भंडारण

संदर्भ –

- Wacquant, L. (2009). Punishing the Poor: The Neoliberal Government of Social Insecurity. Durham: Duke University Press.
- Walby, S. (1990). Theorizing Patriarchy. Oxford: Basil Blackwell.
- Webster, S., Davidson, J., Bifulco, A., Pham, T., & Caretti, V. (2009). European Online Grooming Project : Progress Report Covering Period: 1 June 2009 - 31 December 2009.
- West, C., & Zimmerman, D. (2000). Doing Gender. In M. Kimmel (Ed.), The gendered society reader (pp. 131-149). Oxford: Oxford University Press.
- Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology, 1(1), 1–6.
- Jaishankar, K. (2007). Editorial: Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology, 1(2), 7–9.