2020

Law of Tort

Miss Rubi

Department of law,

Monad University

8/5/2020

Programme-	**LL.B. & B.A. LL.B.**
Course -	**Law of Tort**
Course Code-	**LLB-114**
Sem-	**I & III**
Year-	**2020-21**
Unit-	**1 (Part-3)**
Topic-	**Law Of Tort**
Sub-Topic-	**Cyber Tort**
Faculty-	**Miss Rubi**
E-mail-	**rubysingh109@gmail.com**

साइबरअपकृत्य

साइबर अपकृत्य साइबर दुनिया में नवीनतम और शायद सबसे जटिल समस्या है। "साइबर अपकृत्य को उन प्रजातियों के बारे में कहा जा सकता है, जिनमें से, जीनस पारंपरिक अपकृत्य है, और जहां कंप्यूटर एक वस्तु है या आचरण का विषय है हानि "। “कोई भी आपराधिक गतिविधि जो कंप्यूटर का उपयोग एक साधन के रूप में करती है, लक्ष्य या आगे अपराधों को समाप्त करने के लिए एक साधन साइबर अत्याचार के दायरे में आता है

साइबर अपकृत्य की एक सामान्य परिभाषा "गैरकानूनी कार्य हो सकती है जिसमें कंप्यूटर या तो एक उपकरण या लक्ष्य या दोनों" हो। कंप्यूटर का उपयोग निम्नलिखित प्रकार की गतिविधियों में एक उपकरण के रूप में किया जा सकता है- वित्तीय अपराध, अवैध लेखों की बिक्री, पोर्नोग्राफी, ऑनलाइन जुआ, बौद्धिक संपदा अपराध, ई-मेल स्पूफिंग, जालसाजी, साइबर मानहानि, साइबर स्टाकिंग। हालाँकि, कंप्यूटर निम्नलिखित मामलों में गैरकानूनी कृत्यों के लिए लक्षित हो सकता है- कंप्यूटर / कंप्यूटर सिस्टम / कंप्यूटर नेटवर्क के लिए अनधिकृत पहुँच, इलेक्ट्रॉनिक रूप में निहित जानकारी की चोरी, ई-मेल बमबारी, डेटा डूडलिंग, सलामी हमले, तर्क बम, ट्रोजन हमले , इंटरनेट समय चोरी, वेब जैकिंग, कंप्यूटर सिस्टम की चोरी, कंप्यूटर सिस्टम को शारीरिक रूप से नुकसान पहुंचा रहा है।

➢ इंटरनेट लिटिगेशन का जन्म

इंटरनेट, जिसे अमेरिकी रक्षा विभाग के ARPANET के रूप में शुरू किया गया था, को कंप्यूटर नेटवर्क को विभिन्न रेडियो और उपग्रह नेटवर्क से जोड़ने के लिए डिज़ाइन किया गया था ।.25 इंटरनेट का उल्लेख करने वाली पहली न्यायिक राय संयुक्त राज्य अमेरिका बनाम। Morris.26 मॉरिस में प्रतिवादी एक स्नातक छात्र था। जिसने संयुक्त राज्य अमेरिका में हजारों

विश्वविद्यालय और सैन्य कंप्यूटरों को लकवा मार दिया था। एक ही वर्ष में एक बेल साउथ कंप्यूटर पर अनधिकृत पहुँच प्राप्त करने और टेलीफोन कंपनी की 911 प्रणाली के बारे में मालिकाना जानकारी का दुरुपयोग करने के लिए रॉबर्ट रिग्स पर मुकदमा चलाया गया था। बाद में उसने इस गोपनीय डेटा को हैकर न्यूज़लेटर में प्रकाशित किया।

यह 1994 तक नहीं था कि कोई भी वादी किसी इंटरनेट टोटके के मामले में जीता हो। विवादास्पद निर्णय में, एक मानवविज्ञानी को रिंडोस बनाम हार्डविक में वेस्ट ऑस्ट्रेलिया विश्वविद्यालय में कार्यकाल से वंचित किया गया था। एक प्रतिद्वंद्वी मानवविज्ञानी, हार्डविक ने विश्वविद्यालय के फैसले का समर्थन करते हुए एक बयान पोस्ट किया और रेंडोस पर यौन दुर्व्यवहार का आरोप लगाते हुए और ऑस्ट्रेलिया के आदिवासी लोगों के लिए हानिकारक अनुसंधान का आरोप लगाया। हालांकि एक ऑस्ट्रेलियाई अदालत ने एक इंटरनेट टार्चर मामले में इस पहले नुकसान के पुरस्कार का आकलन किया, जिसमें अधिकांश बहुमत थे। बाद में अमेरिका में साइबर ट्राउट प्रज्जवलित किए गए हैं। पिछले एक दशक के दौरान, अमेरिकी अत्याचार कानून इंटरनेट की बदनामी, ई-मेल स्टैकिंग, स्पैमिंग, और वेब साइटों पर अतिचार जैसे ऑनलाइन चोटों को दूर करने के लिए विकसित होने लगा है।

- **पारंपरिक अपकृत्य और साइबर अपकृत्य बीच अंतर**

जाहिरा तौर पर साइबर और पारंपरिक अपकृत्य के बीच कोई अंतर नहीं है। हालांकि एक गहरी आत्मनिरीक्षण पर हम कह सकते हैं कि पारंपरिक और साइबर अपकृत्य के बीच सीमांकन की एक अच्छी रेखा मौजूद है, जो प्रशंसनीय है। सीमांकन साइबर अत्याचार के मामलों में माध्यम की भागीदारी में निहित है। साइबर टोट के लिए साइन क्वालिफिकेशन नॉन यह है कि वर्चुअल साइबर मीडियम i, e के किसी भी स्तर पर एक भागीदारी होनी चाहिए। साइबर स्पेस।

- **साइबर अपकृत्य की संभावना के कारण:**

हार्ट ने अपने कार्य "कानून की अवधारणा" में कहा है कि 'मानव कमजोर हैं इसलिए उनकी रक्षा के लिए कानून का शासन आवश्यक है'। साइबरस्पेस पर इसे लागू करते हुए हम कह सकते हैं कि कंप्यूटर असुरक्षित हैं, इसलिए साइबर अत्याचार से बचाव और उनकी सुरक्षा के लिए कानून का शासन आवश्यक है। कंप्यूटर की भेद्यता के कारणों को कहा जा सकता है:

1. तुलनात्मक रूप से छोटे स्थान में डेटा स्टोर करने की क्षमता- कंप्यूटर में बहुत कम जगह में डेटा संग्रहीत करने की अनूठी विशेषता है। यह भौतिक या आभासी माध्यम से जानकारी निकालने या प्राप्त करने के लिए बहुत अधिक आसान बनाता है।

2. उपयोग करने में आसान-अनधिकृत पहुंच से कंप्यूटर सिस्टम की रखवाली में आने वाली समस्या यह है कि इसमें मानवीय त्रुटि के कारण नहीं बल्कि जटिल तकनीक के कारण उल्लंघन की पूरी संभावना है। गुप्त रूप से प्रत्यारोपित लॉजिक बम, कुंजी लकड़हारा जो एक्सेस कोड, उन्नत वॉयस रिकॉर्डर चुरा सकता है; रेटिना इमेजर्स आदि जो बायोमेट्रिक सिस्टम को बेवकूफ बना सकते हैं और फायरवॉल को बायपास किया जा सकता है, को कई सुरक्षा प्रणाली से गुजारा जा सकता है।

3. सिस्टम की जटिलता-कंप्यूटर ऑपरेटिंग सिस्टम पर काम करते हैं और बदले में ये ऑपरेटिंग सिस्टम लाखों कोड से बने होते हैं। मानव मन पतनशील है और यह संभव नहीं है कि किसी भी स्तर पर चूक न हो। इन लुकासाना का फायदा उठाया जा सकता है और कंप्यूटर सुरक्षा प्रणालियों में प्रवेश किया जा सकता है।

4. लापरवाही- लापरवाही मानव आचरण के साथ बहुत निकटता से जुड़ा हुआ है। इसलिए यह बहुत संभावना है कि कंप्यूटर सिस्टम की सुरक्षा करते समय कोई लापरवाही हो सकती है, जो बदले में पहुंच और नियंत्रण प्राप्त करने के लिए एक लूप होल प्रदान करता है और बदले में कंप्यूटर सिस्टम का दुरुपयोग करता है।

5. साक्ष्य का नुकसान- साक्ष्य का खोना एक बहुत ही सामान्य और स्पष्ट समस्या है क्योंकि सभी डेटा नियमित रूप से नष्ट हो जाते हैं क्योंकि वे हर पल अपडेट होते रहते हैं। क्षेत्रीय सीमा के बाहर डेटा का आगे संग्रह भी जांच की इस प्रणाली को पंगु बना देता है।

➢ साइबर अपकृत्य करने का तरीका

1. कंप्यूटर सिस्टम या नेटवर्क / हैकिंग के लिए अनधिकृत पहुँच-इस तरह के अपराध को सामान्य रूप से हैकिंग कहा जाता है। हालाँकि सूचना प्रौद्योगिकी अधिनियम 2002 के फ्रैमर्स ने इस शब्द का उपयोग नहीं किया है और "अनधिकृत पहुँच" शब्द का "हैकिंग" शब्द की तुलना में व्यापक अर्थ है।

2. इलेक्ट्रॉनिक रूप में निहित जानकारी की चोरी-इसमें कंप्यूटर हार्ड डिस्क, रिमूवेबल स्टोरेज मीडिया, मैग्नेटिक डिस्क, फ्लैश मेमोरी डिवाइस आदि में संग्रहीत जानकारी शामिल होती है। चोरी या तो डेटा को विनियोजित करके या डेटा को गलत तरीके से जोड़कर या आभासी माध्यम से छेड़छाड़ करके हो सकती है। मध्यम।

3. ईमेल बॉम्बिंग- इस तरह की गतिविधि पीड़ित को बड़ी संख्या में मेल भेजने को संदर्भित करती है, जो एक व्यक्ति या कंपनी या यहां तक कि मेल सर्वर हो सकता है जिसके परिणामस्वरूप दुर्घटनाग्रस्त हो सकता है।

4. डेटा डीडलिंग- इस तरह के हमले में कंप्यूटर को संसाधित करने से पहले कच्चे डेटा में फेरबदल करना और प्रसंस्करण पूरा होने के बाद इसे वापस बदलना शामिल है। विद्युत बोर्ड को डेटा डीडलिंग की समान समस्या का सामना करना पड़ा, जबकि विभाग को कम्प्यूटरीकृत किया जा रहा था।

5. सलामी हमले- इस तरह के अपराध आमतौर पर वित्तीय संस्थानों में या वित्तीय अपराधों को अंजाम देने के लिए प्रचलित हैं। इस प्रकार के अपराध की एक महत्वपूर्ण विशेषता यह है कि परिवर्तन इतना छोटा है कि यह सामान्य रूप से किसी का ध्यान नहीं जाएगा। उदाहरण के लिए ज़िग्लर मामला जिसमें बैंक के सिस्टम में एक लॉजिक बम पेश किया गया था, जिसने हर खाते से 10 सेंट काट लिए और उसे एक विशेष खाते में जमा कर दिया।

6. सेवा हमले से इनकार- पीड़ित का कंप्यूटर अधिक अनुरोधों से भरा हुआ है, क्योंकि यह दुर्घटना का कारण बन सकता है। डिस्ट्रीब्यूटेड डेनियल ऑफ सर्विस (DDoS) हमला भी सेवा हमले का एक प्रकार का खंडन है, जिसमें अपराधी संख्या में व्यापक और व्यापक होते हैं। जैसे अमेज़न, याहू।

7. वायरस / कृमि के हमले- वायरस ऐसे प्रोग्राम हैं जो खुद को कंप्यूटर या फाइल से जोड़ते हैं और फिर एक नेटवर्क पर अन्य फाइलों और अन्य कंप्यूटरों में खुद को प्रसारित करते हैं। वे आमतौर पर कंप्यूटर पर डेटा को प्रभावित करते हैं, या तो इसे बदलकर या हटाकर। कीड़े, वायरस के विपरीत मेजबान को खुद को संलग्न करने की आवश्यकता नहीं है। वे केवल स्वयं की कार्यात्मक प्रतियां बनाते हैं और ऐसा बार-बार करते हैं जब तक कि वे कंप्यूटर की मेमोरी पर सभी उपलब्ध स्थान को नहीं खा लेते हैं। एग प्यार बग वायरस, जो दुनिया के कम से कम 5% कंप्यूटरों को प्रभावित करता है। नुकसान का हिसाब $ 10 मिलियन था। दुनिया का सबसे प्रसिद्ध कीड़ा था इंटरनेट वर्म, जिसने 1988 में रॉबर्ट मॉरिस द्वारा इंटरनेट पर कुछ समय के लिए ढीला कर दिया, जिसने इंटरनेट के विकास को लगभग पूरी तरह से रोक दिया।

8. लॉजिक बम- ये इवेंट डिपेंडेंट प्रोग्राम हैं। इसका तात्पर्य यह है कि ये कार्यक्रम केवल कुछ करने के लिए बनाए जाते हैं जब एक निश्चित घटना (ट्रिगर इवेंट के रूप में जाना जाता है) होती है। उदाहरण के लिए, कुछ वायरस को लॉजिक बम भी कहा जा सकता है क्योंकि वे पूरे वर्ष में निष्क्रिय रहते हैं और केवल एक विशेष तिथि (चेरनोबिल वायरस की तरह) पर सक्रिय हो जाते हैं।

9. ट्रोजन हमले- इस शब्द का मूल शब्द 'ट्रोजन हॉर्स' है। सॉफ्टवेयर क्षेत्र में इसका मतलब एक अनधिकृत कार्यक्रम है, जो एक अधिकृत कार्यक्रम के रूप में खुद का प्रतिनिधित्व करके किसी अन्य की प्रणाली पर नियंत्रण प्राप्त करता है। ट्रोजन को स्थापित करने का सबसे आम रूप ई-मेल के माध्यम से है। जैसे कि अमेरिका में एक महिला फिल्म निर्देशक के कंप्यूटर में एक ट्रोजन को चैटिंग के दौरान स्थापित किया गया था। कंप्यूटर में स्थापित वेब कैम के माध्यम से साइबर अपराधी ने उसकी नग्न तस्वीरें प्राप्त कीं। उसने इस महिला को और परेशान किया।

10. इंटरनेट समय की चोरी- आम तौर पर इस प्रकार की चोरी में पीड़ित व्यक्ति का इंटरनेट सर्फिंग घंटे किसी अन्य व्यक्ति द्वारा उपयोग किया जाता है। यह लॉगिन आईडी और पासवर्ड तक पहुंच प्राप्त करके किया जाता है। उदा। कर्नल बाजवा का मामला- इंटरनेट के घंटे किसी अन्य व्यक्ति द्वारा उपयोग किए जाते थे। यह शायद भारत में साइबर अपराध से संबंधित पहले रिपोर्ट किए गए मामलों में से एक था। हालाँकि इस मामले ने पुलिस को बदनाम कर दिया, क्योंकि साइबर अत्याचार की प्रकृति को समझने में उनकी कमी थी।

11. वेब जैकिंग-यह शब्द हाय जैकिंग शब्द से लिया गया है। इस तरह के अपराधों में हैकर दूसरे की वेब साइट पर पहुंच और नियंत्रण हासिल करता है। वह साइट पर जानकारी को बदल या बदल भी सकता है। यह राजनीतिक उद्देश्यों को पूरा करने या पैसे के लिए किया जा सकता है। उदाहरण के लिए हाल ही में एमआईटी (सूचना प्रौद्योगिकी मंत्रालय) के मामले में पाकिस्तानी हैकर्स द्वारा उसकी साइट को हैक कर लिया गया और कुछ अश्लील मामले को उसमें रखा गया। इसके अलावा बॉम्बे क्राइम ब्रांच की साइट भी वेब जैकेड थी। वेब जैकिंग का एक और मामला 'गोल्ड फिश केस' का है। इस मामले में साइट को हैक कर लिया गया था और सोने की मछली से संबंधित जानकारी बदल दी गई थी। इसके अलावा 1 मिलियन अमेरिकी डॉलर की फिरौती की मांग की गई थी। इस प्रकार वेब जैकिंग एक ऐसी प्रक्रिया है जहां किसी अन्य की साइट पर नियंत्रण इसके लिए कुछ विचार द्वारा समर्थित किया जाता है।

आम तौर पर साइबर अपराधी कौन होते हैं:

साइबर अपराधी विभिन्न समूहों / श्रेणी के होते हैं। यह विभाजन उस वस्तु के आधार पर उचित हो सकता है जो उनके दिमाग में है। साइबर अपराधियों की श्रेणी निम्नलिखित हैं-

1. 6-18 वर्ष के आयु वर्ग के बीच के बच्चे और किशोर - बच्चों में इस प्रकार के विलक्षण व्यवहार पैटर्न का सरल कारण ज्यादातर चीजों को जानने और जानने की जिज्ञासा के कारण देखा जाता है। अन्य संज्ञानात्मक कारण हो सकता है कि वे अपने समूह के अन्य बच्चों के बीच खुद को उत्कृष्ट साबित करें। इसके अलावा कारण मनोवैज्ञानिक भी हो सकते हैं। उदाहरण के लिए, बाल भारती (दिल्ली) का मामला उनके दोस्तों द्वारा किए गए अपराध के उत्पीड़न का परिणाम था।

2. संगठित हैकर्स-इस प्रकार के हैकर्स ज्यादातर कुछ उद्देश्य पूरा करने के लिए एक साथ आयोजित किए जाते हैं। इसका कारण उनके राजनीतिक पूर्वाग्रह, कट्टरवाद आदि को पूरा करना हो सकता है। हाल ही में भारत सरकार को उसी के साथ लक्षित किया गया था। इसके अलावा नासा के साथ-साथ Microsoft साइटों पर भी हैकरों का हमला होता रहता है।

3. पेशेवर हैकर्स / पटाखे - उनका काम पैसे के रंग से प्रेरित है। इस प्रकार के हैकर्स ज्यादातर प्रतिद्वंद्वियों की साइट को हैक करने और विश्वसनीय, विश्वसनीय और मूल्यवान जानकारी प्राप्त करने के लिए नियोजित होते हैं। इसके अलावा, वे नियोक्ता की प्रणाली को मूल रूप से खामियों का पता लगाकर इसे सुरक्षित बनाने के उपाय के रूप में क्रैक करने के लिए कार्यरत हैं।

राज्य डेटाबेस और समाचार सेवाएं, 41 (3) लॉ फर्मों के साइबरस्पेस रिसर्च लाइब्रेरी, 42 (4) राष्ट्रीय, क्षेत्रीय और स्थानीय फैसले के रिपोर्टर, डोमेन नाम विवादों की 43 (5) रिपोर्ट, 44 (6) व्यक्तिगत

साइबर मामलों के कानून पर रिपोर्ट किए गए फर्म वेब साइटें, 45 (7) लॉ स्कूल रिसर्च सेंटर, 46 (8) अमेरिकन लॉ रिपोर्ट्स ("एएलआर") एनोटेशन, 47 (9) सभी इंटरनेट से संबंधित मैले प्रकाशन, 48 (10) ई-कॉमर्स लॉ सेकेंडरी स्रोत, 49 (11) इंटरनेट

- **साइबर अपकृत्य का एक व्यापक वर्गीकरण**:

1. ई-मेल के माध्यम से उत्पीड़न-ई-मेल के माध्यम से उत्पीड़न कोई नई अवधारणा नहीं है। यह पत्रों के माध्यम से परेशान करने के समान है। हाल ही में मुझे एक महिला का मेल मिला था जिसमें उसने उसी के बारे में शिकायत की थी। उसका पूर्व बॉय फ्रेंड उसे कभी-कभी भावनात्मक रूप से ब्लैकमेल कर रहा था और उसे धमकी भी दे रहा था। यह ई-मेल के माध्यम से उत्पीड़न का एक बहुत ही सामान्य प्रकार है।

2. साइबर-स्टैकिंग- ऑक्सफोर्ड डिक्शनरी ने पीछा करने को "चुपके से पीछा करने" के रूप में परिभाषित किया है। साइबर स्टैकिंग में पीड़ित द्वारा बार-बार बुलेटिन बोर्डों पर संदेश पोस्ट करना (कभी-कभी धमकी देना), इंटरनेट पर एक व्यक्ति के आंदोलनों का अनुसरण करना शामिल है, जिसमें पीड़ित द्वारा बार-बार चैट रूम में प्रवेश करना, लगातार ईमेल आदि से पीड़ित को बम से उड़ाना आदि।

3. अश्लील सामग्री / अश्लील प्रदर्शन / अश्लीलता (मूल रूप से बाल पोर्नोग्राफी) का प्रसार / अश्लील प्रदर्शन के माध्यम से प्रदूषण - नेट पर अश्लीलता के विभिन्न रूप हो सकते हैं। इसमें इन निषिद्ध सामग्रियों से युक्त वेब साइट की मेजबानी शामिल हो सकती है। इन अश्लील सामग्रियों के उत्पादन के लिए कंप्यूटर का उपयोग। इंटरनेट के माध्यम से डाउनलोड करना, अश्लील सामग्री। ये अश्लील मामले किशोरों के दिमाग को नुकसान पहुंचा सकते हैं और उनके दिमाग को खराब या भ्रष्ट कर सकते हैं। अश्लील साहित्य के दो ज्ञात मामले हैं दिल्ली बाल भारती का मामला और बॉम्बे का मामला जिसमें दो स्विस दंपति ने झुग्गी के बच्चों को अश्लील तस्वीरों के लिए मजबूर किया। मुंबई पुलिस ने बाद में उन्हें गिरफ्तार कर लिया।

4. मानहानि: -यह किसी भी व्यक्ति को आम तौर पर समाज के सही सोच वाले सदस्यों के अनुमान में व्यक्ति को कम करने या उसे दूर करने या उससे बचने या घृणा, अवमानना या उपहास करने के लिए उसे उजागर करने के लिए प्रेरित करने का एक कार्य है। एक वर्चुअल माध्यम की भागीदारी को छोड़कर साइबर मानहानि पारंपरिक मानहानि से अलग नहीं है। जैसे कि रोहित का मेल अकाउंट हैक कर लिया गया था और कुछ मेल्स उसके अकाउंट से उसके कुछ बैच मेट्स को भेज दिए गए थे ताकि वो किसी लड़की के साथ उसके अफेयर के बारे में बता सके।

5. अनधिकृत नियंत्रण / कंप्यूटर प्रणाली पर पहुंच: -इस गतिविधि को सामान्यतः हैकिंग कहा जाता है। भारतीय कानून ने हालांकि, शब्द हैकिंग को एक अलग अर्थ दिया है, इसलिए हम भ्रम को रोकने के लिए "हैकिंग" शब्द के साथ "अनधिकृत पहुंच" शब्द का उपयोग नहीं करेंगे, क्योंकि हैकिंग की तुलना में 2000 के अधिनियम में प्रयुक्त शब्द बहुत व्यापक है।

6. ई मेल स्पूफिंग-एक स्पूफिंग ई-मेल को एक कहा जा सकता है, जो इसके मूल को गलत तरीके से प्रस्तुत करता है। यह दर्शाता है कि यह मूल है जिससे यह वास्तव में उत्पन्न होता है, भिन्न होता है। हाल ही में स्पूफ किए गए मेलों को श्री ना.विजयशंकर (naavi.org) के नाम पर भेजा गया, जिसमें वायरस था। इंडियाना के पर्ड्यू विश्वविद्यालय में स्नातक छात्र राजेश मनार को कॉलेज परिसर में एक परमाणु उपकरण को विस्फोट करने की धमकी देने के आरोप में गिरफ्तार किया गया था। कथित ई-मेल दूसरे छात्र के खाते से छात्र सेवाओं के लिए उपाध्यक्ष को भेजा गया था। हालाँकि वह मेल राजेश मानार के खाते से भेजा गया था।

7. कंप्यूटर बर्बरता: -बर्बरता का अर्थ है जानबूझकर दूसरे की संपत्ति को नष्ट करना या नुकसान पहुंचाना। इस प्रकार कंप्यूटर बर्बरता किसी भी व्यक्ति के कंप्यूटर को किसी भी तरह के शारीरिक नुकसान के दायरे में शामिल कर सकती है। ये हरकतें कंप्यूटर की चोरी, कंप्यूटर का कुछ हिस्सा या कंप्यूटर से जुड़ी एक परिधि या कंप्यूटर या इसके बाह्य उपकरणों को शारीरिक रूप से क्षतिग्रस्त करने का रूप ले सकती हैं।

8. बौद्धिक संपदा अपराध / पायरेटेड सॉफ्टवेयर का वितरण: -बौद्धिक संपदा में अधिकारों का एक समूह होता है। कोई भी गैरकानूनी कार्य जिसके द्वारा मालिक अपने अधिकारों से पूरी तरह या आंशिक रूप से वंचित है, एक अपराध है। आईपीआर उल्लंघन के सामान्य रूप को सॉफ्टवेयर पाइरेसी, कॉपीराइट उल्लंघन, ट्रेडमार्क और सर्विस मार्क उल्लंघन, कंप्यूटर सोर्स कोड की चोरी आदि कहा जा सकता है। हैदराबाद कोर्ट ने एक लैंड मार्क फैसले में तीन लोगों को दोषी ठहराया है और उन्हें छह महीने की सजा सुनाई है अनधिकृत नकल और पायरेटेड सॉफ्टवेयर की बिक्री के लिए प्रत्येक को कारावास और 50,000 का जुर्माना।

9. सरकारी संगठन के खिलाफ साइबर आतंकवाद: -इस मोड़ पर एक आवश्यकता महसूस की जा सकती है कि साइबर आतंकवाद और साइबर तनाव के बीच अंतर करने की आवश्यकता क्या है। दोनों खतरनाक कृत्य हैं। हालाँकि इन दोनों कृत्यों के बीच अंतर करने की एक अनिवार्य आवश्यकता है। साइबर अत्याचार आम तौर पर एक घरेलू मुद्दा है, जिसके अंतरराष्ट्रीय परिणाम हो सकते हैं, हालांकि साइबर आतंकवाद एक वैश्विक चिंता है, जिसके घरेलू होने के साथ-साथ अंतर्राष्ट्रीय परिणाम भी हैं। इंटरनेट पर इन आतंकवादी हमलों का सामान्य रूप सेवा के हमलों, घृणा फैलाने वाली वेबसाइटों और घृणास्पद ईमेल, संवेदनशील कंप्यूटर नेटवर्क पर हमले आदि को वितरित करने से है। प्रौद्योगिकी प्रेमी आतंकवादी 512-बिट एन्क्रिप्शन का उपयोग कर रहे हैं, जो डिक्रिप्ट करना असंभव है। हाल के उदाहरण का हवाला दिया जा सकता है - ओसामा बिन लादेन, लिट्टे, इराक युद्ध के दौरान अमेरिका की सेना की तैनाती प्रणाली पर हमला।

साइबर आतंकवाद को "सामाजिक गतिविधियों, वैचारिक, धार्मिक, राजनीतिक या इसी तरह के उद्देश्यों के लिए, या ऐसे उद्देश्यों की पूर्ति में किसी भी व्यक्ति को डराने-धमकाने के उद्देश्य से, साइबर स्पेस में विघटनकारी गतिविधियों, या इसके खतरे के पूर्व निर्धारित उपयोग" के रूप में परिभाषित किया जा सकता है। “

एक और परिभाषा के तहत साइबर आतंकवाद के प्रत्येक अधिनियम को अपने दायरे में शामिल करने का प्रयास किया जा सकता है।

आतंकवादी का अर्थ है, वह व्यक्ति जो व्यक्तियों की हत्या या हिंसा में या सेवाओं के विघटन में या समुदाय के लिए आवश्यक संचार के साधनों के लिए या संपत्ति को नुकसान पहुंचाने के लिए

- जनता या जनता के किसी भी वर्ग को शामिल करता है। डर; या
- विभिन्न धार्मिक, नस्लीय, भाषा या क्षेत्रीय समूहों या जातियों या समुदायों के बीच प्रतिकूलता को प्रभावित करना; या
- कानून द्वारा स्थापित सरकार के साथ ज़बरदस्ती करना या उसे खत्म करना; या
- राष्ट्र की संप्रभुता और अखंडता को खतरे में डालना और एक साइबर आतंकवादी वह व्यक्ति है जो उपरोक्त उद्देश्यों को प्राप्त करने के लिए कंप्यूटर सिस्टम को एक साधन के रूप में उपयोग करता है या समाप्त करता है। इसके बाद किया गया हर कार्य साइबर आतंकवाद का एक कार्य है।

10. तस्करी: - तस्करी विभिन्न रूपों को मान सकती है। यह ड्रग्स, इंसानों, हथियारों के हथियारों आदि की तस्करी हो सकती है। तस्करी के ये रूप अनियंत्रित हो रहे हैं क्योंकि उन्हें छद्म धर्म के तहत किया जाता है। चेन्नई में एक रैकेट का भंडाफोड़ हुआ जहां शहद के छद्म नाम से ड्रग्स बेचे जा रहे थे।

11. धोखाधड़ी और धोखा: -ऑनलाइन धोखाधड़ी और धोखाधड़ी सबसे आकर्षक व्यवसायों में से एक है जो आज साइबर स्पेस में बढ़ रहे हैं। यह विभिन्न रूपों को मान सकता है। ऑनलाइन धोखाधड़ी और धोखाधड़ी के कुछ मामले जो प्रकाश में आए हैं, वे हैं क्रेडिट कार्ड से संबंधित अपराध, संविदात्मक अपराध, नौकरी की पेशकश, आदि। हाल ही में मेट्रोपोलिटन मजिस्ट्रेट दिल्ली (17) की अदालत ने 24 वर्षीय एक इंजीनियर को दोषी पाया एक कॉल सेंटर में, कैम्पा के क्रेडिट कार्ड का विवरण प्राप्त करने के लिए धोखाधड़ी की और सोनी वेबसाइट से एक टेलीविजन और एक तारहित फोन खरीदा। मेट्रोपोलिटन मजिस्ट्रेट गुलशन कुमार ने अजीम को आईपीसी के तहत धोखाधड़ी के लिए दोषी

ठहराया, लेकिन उसे जेल नहीं भेजा। इसके बजाय, अजीम को 20,000 रुपये का निजी बांड प्रस्तुत करने के लिए कहा गया, और एक साल की परिवीक्षा पर रिहा किया गया।

- **साइबर अपराध और साइबर हमले के बीच अंतर**

साइबर क्राइम और साइबर टॉर्ट्स के बीच विशिष्ट अंतर है, जिसे क्लियर करना होगा जब हम साइबर ट्रेट्स पर चर्चा कर रहे हैं।साइबर अपराध में हैकिंग / क्रैकिंग, अनधिकृत सूचनाओं का कब्ज़ा, सरकारी संगठनों के खिलाफ साइबर आतंकवाद, पायरेटेड सॉफ़्टवेयर का वितरण, ईमेल के माध्यम से उत्पीड़न, साइबर पीछा, इंटरनेट पर अश्लील सामग्री का प्रसार, मानहानि, हैकिंग / क्रैकिंग, अश्लील प्रदर्शन, कंप्यूटर बर्बरता शामिल हैं। , संचारण वायरस, इंटरनेट घुसपैठ, कंप्यूटर सिस्टम, पोर्नोग्राफी पर अनधिकृत नियंत्रण, युवाओं को अश्लील सामग्री, ट्रैफिकिंग को उजागर करना।

साइबर टॉर्ट्स में साइबर स्टैकिंग, गोपनीयता का उल्लंघन, साइबर अश्लीलता और साइबर मानहानि शामिल हैं।तो कुछ ऐसे तत्व हो सकते हैं जो दोनों में सामान्य हो सकते हैं लेकिन दोनों के बीच कई अंतर हैं।

- **वैधानिक प्रावधान:**

भारतीय संसद ने उस प्रस्ताव को प्रभावी करने के लिए आवश्यक माना जिसके द्वारा महासभा ने संयुक्त राष्ट्र आयोग द्वारा व्यापार कानून पर अपनाए गए इलेक्ट्रॉनिक वाणिज्य पर मॉडल कानून को अपनाया। जिसके परिणामस्वरूप 17 मई 2000 को सूचना प्रौद्योगिकी अधिनियम 2000 पारित किया गया और लागू किया गया। इस अधिनियम की प्रस्तावना में ई-कॉमर्स को वैध बनाने और भारतीय दंड संहिता 1860, भारतीय साक्ष्य अधिनियम 1872, बैंकर बुक को संशोधित करने के अपने उद्देश्य के बारे में बताया गया है। साक्ष्य अधिनियम 1891 और भारतीय रिज़र्व बैंक अधिनियम 1934। इन अधिनियमों में बदलाव को शामिल करने का मूल उद्देश्य उन्हें 2000 के अधिनियम के अनुरूप बनाना है। ताकि वे प्रभावी तरीके से साइबर दुनिया के मामलों को नियंत्रित और नियंत्रित कर सकें।

महत्वपूर्ण अनुभाग एस.एस. 43,65,66,67। अनधिकृत पहुंच, अनधिकृत डाउनलोडिंग, वायरस के हमलों या किसी भी संदूषक के साथ विशेष रूप से धारा 43 में क्षति, विघटन, पहुंच से इनकार, किसी व्यक्ति द्वारा प्राप्त सेवा के साथ हस्तक्षेप का कारण बनता है। यह अनुभाग रु। उपाय के द्वारा 1 करोड़। धारा 65 'कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़' से संबंधित है और 3 साल तक कारावास या जुर्माने का प्रावधान है, जो 2 साल या दोनों तक हो सकता है। धारा 66 'कंप्यूटर सिस्टम के साथ हैकिंग' से संबंधित है और 3 साल तक कारावास या जुर्माने का प्रावधान है, जो 2 साल या दोनों तक का हो सकता है। आगे की धारा 67 में अश्लील सामग्री के प्रकाशन से संबंधित है और 10 वर्ष की अवधि तक कारावास और रुपये तक के जुर्माने का प्रावधान है। 2 लाख।

एक साइबर अपकृत्य का अनुकूलन

बॉम्बे हाई कोर्ट के निर्देशों पर केंद्र सरकार ने दिनांक 25.03.03 की एक अधिसूचना द्वारा निर्णय लिया है कि प्रत्येक राज्य में सूचना प्रौद्योगिकी विभाग के सचिव को पदनाम द्वारा प्रत्येक राज्य के लिए एओ नियुक्त किया जाएगा।

भारतीय कानून के तहत बिचौलियों और लेखक की देयता

इंटरनेट ने दुनिया भर में एक बड़ी राशि और विभिन्न प्रकार की जानकारी फैलाने के लिए पहले से कहीं अधिक आसान बना दिया है। जैसा कि पहले उल्लेख किया गया है, SNW एक जमीनी स्तर पर, लोगों के बीच सूचनाओं के आदान-प्रदान के लिए एक माध्यम है। एसएनडब्ल्यू किसी भी व्यक्ति को अपने स्वयं के या किसी तीसरे व्यक्ति की आभासी प्रोफ़ाइल पर मानहानि सहित किसी भी बयान को लिखने की अनुमति देता है। इस परिदृश्य में, स्वाभाविक रूप से जो सवाल उठता है: उस व्यक्ति के खिलाफ मुकदमा दायर किया जा सकता है जिसके खिलाफ ऐसा मानहानि करने वाला बयान दिया गया है।

ऑपरेटिव भारतीय कानून के तहत, जिस व्यक्ति ने इस तरह के बयान के साथ-साथ इसके वितरक और प्रकाशकों पर भी मुकदमा किया हो, उस पर मुकदमा चलाया जा सकता है। ऐसे बयान के लेखक के अलावा, संबंधित SNW, वेबसाइट धारक, इंटरनेट सेवा प्रदाता, साथ ही ऐसे SNW के अन्य उपयोगकर्ता जिनके प्रोफाइल पर अपमानजनक बयान लेखक द्वारा लिखे गए हैं, के रूप में बिचौलियों को उनके खिलाफ मुकदमा दायर किया जा सकता है। मानहानि वाले बयानों के प्रकाशक के रूप में क्षमता और ऐसे बयानों के लिए उत्तरदायी ठहराया जा सकता है। यह ध्यान दिया जाना चाहिए कि ऐसे बिचौलियों या एसएनडब्ल्यू के अन्य उपयोगकर्ताओं को अपने स्वयं के आभासी प्रोफ़ाइल पर लेखक द्वारा ऐसे मानहानिकारक बयानों के बारे में पता नहीं हो सकता है।

सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 79

("अधिनियम") नेटवर्क सेवा प्रदाताओं को प्रतिरक्षा प्रदान करता है। अधिनियम की धारा 79 के अनुसार, एक 'नेटवर्क सेवा प्रदाता' (एक ऐसे व्यक्ति के रूप में परिभाषित किया जाता है जो किसी अन्य व्यक्ति की ओर से इलेक्ट्रॉनिक संदेशों को प्राप्त करता है, संग्रहीत करता है या प्रसारित करता है) अधिनियम, या नियमों या नियमों के तहत उत्तरदायी नहीं होगा, के तहत, किसी भी तीसरे पक्ष की जानकारी या उसके द्वारा उपलब्ध कराए गए डेटा के लिए यदि वह साबित करता है कि अपराध या उल्लंघन उसकी जानकारी के बिना किया गया था या उसने इस तरह के अपराध या उल्लंघन के कमीशन को रोकने के लिए सभी उचित परिश्रम का अभ्यास किया था।

सूचना प्रौद्योगिकी संशोधन अधिनियम, 2008

सूचना प्रौद्योगिकी संशोधन अधिनियम, 2008 भारतीय संसद द्वारा 22 दिसंबर, 2008 को पारित किया गया था और राष्ट्रपति के आश्वासन के बाद, यह 5 फरवरी, 2009 से एक कानून बन गया है। संशोधन संयुक्त राज्य अमेरिका में प्रचलित कानून के लिए समानता की एक निश्चित डिग्री है अमेरिका ("यूएसए")। संयुक्त राज्य अमेरिका में, बिचौलियों जैसे एसएनडब्ल्यू, इंटरनेट सेवा प्रदाताओं और अन्य इंटरैक्टिव वेब सेवा प्रदाताओं को मानहानि के तहत देयता से छूट दी जाती

है यदि (i) वे साबित करते हैं कि उनका बयान या सामग्री पर कोई नियंत्रण नहीं है और (ii) वे इस तरह के बयान या सामग्री को हटाते हैं वादी से नोटिस मिलने पर तुरंत उनकी वेबसाइट या नेटवर्क।

इस संशोधन अधिनियम की संशोधित धारा 79 संयुक्त राज्य अमेरिका के कानून के बराबर व्यवस्था प्रदान करती है। सूचना प्रौद्योगिकी अधिनियम के प्रासंगिक प्रावधान निम्नलिखित हैं (उक्त संशोधन लागू होने के बाद)।

धारा 79:

(1) लागू होने के समय किसी भी अन्य कानून में निहित कुछ के बावजूद, लेकिन उप-वर्गों (2) और (3) के प्रावधानों के अधीन, एक मध्यस्थ किसी भी तीसरे पक्ष की जानकारी, डेटा, के लिए उत्तरदायी नहीं होगा या संचार लिंक उसके द्वारा उपलब्ध कराया गया।

(2) उप-धारा (1) के प्रावधान लागू होंगे यदि -

(ए) मध्यस्थ का कार्य एक संचार प्रणाली तक पहुंच प्रदान करने तक सीमित है, जिस पर तीसरे पक्ष द्वारा उपलब्ध कराई गई जानकारी प्रेषित या अस्थायी रूप से संग्रहीत होती है; या

(बी) मध्यस्थ नहीं है-

(i) ट्रांसमिशन आरंभ करें,

(ii) ट्रांसमिशन के रिसीवर का चयन करें, और

(iii) ट्रांसमिशन में निहित जानकारी का चयन करें या संशोधित करें।

(3) उप-धारा (1) के प्रावधान लागू नहीं होंगे यदि -

(क) मध्यस्थ ने गैरकानूनी अधिनियम के कमीशन में साजिश रची या समाप्त कर दी है;

(ख) वास्तविक ज्ञान प्राप्त करने पर, या उपयुक्त सरकार या उसकी एजेंसी द्वारा सूचित किए जाने पर कि मध्यस्थ द्वारा नियंत्रित कंप्यूटर संसाधन से संबंधित या उससे जुड़ी किसी भी जानकारी, डेटा या संचार लिंक का इस्तेमाल गैरकानूनी कार्य करने के लिए किया जा रहा है, मध्यस्थ किसी भी तरीके से सबूतों को मिटाए बिना उस संसाधन पर उस सामग्री तक त्वरित रूप से पहुंच या अक्षम करने में विफल रहता है।

(4) मध्यस्थ इस तरह के अन्य दिशानिर्देशों का पालन करेगा क्योंकि केंद्र सरकार इस संबंध में लिख सकती है।

स्पष्टीकरण ।-- इस खंड के प्रयोजन के लिए, अभिव्यक्ति "तीसरे पक्ष की जानकारी" का अर्थ है किसी मध्यस्थ द्वारा मध्यस्थ के रूप में उसकी क्षमता से निपटा गया कोई भी जानकारी।

धारा 2 (डब्ल्यू) -

"मध्यस्थ", किसी विशेष इलेक्ट्रॉनिक रिकॉर्ड के संबंध में, किसी भी व्यक्ति का अर्थ है जो किसी अन्य व्यक्ति की ओर से उस रिकॉर्ड को प्राप्त करता है, संग्रहीत करता है या प्रसारित करता है या उस रिकॉर्ड के संबंध में कोई सेवा प्रदान करता है और इसमें दूरसंचार सेवा प्रदाता, नेटवर्क शामिल हैं सेवा प्रदाताओं, इंटरनेट सेवा प्रदाताओं, वेब होस्टिंग सेवा प्रदाताओं, खोज इंजन,

ऑनलाइन भुगतान साइटों, ऑनलाइन नीलामी साइटों, ऑनलाइन बाजार स्थानों और साइबर कैफे,लेकिन धारा 43 ए में संदर्भित बॉडी कॉर्पोरेट शामिल नहीं है। "

- **वैधानिक प्रावधानों का विश्लेषण:**

सूचना प्रौद्योगिकी अधिनियम 2000 निस्संदेह ऐसे समय में एक स्वागत योग्य कदम था जब इस विशेष क्षेत्र पर कोई कानून नहीं था। हालांकि अधिनियम ने अपने आवेदन के दौरान कुछ हद तक अपर्याप्त साबित किया है। अधिनियम में विभिन्न खामियां हैं-

1. वह कानून जिसमें पर्याप्त सार्वजनिक बहस के बिना कानून पारित किया गया था, वास्तव में वांछित उद्देश्य की पूर्ति नहीं किया गया। विशेषज्ञों की राय है कि कानून की अपर्याप्तता के कारणों में से एक है जल्दबाजी जिसमें इसे संसद द्वारा पारित किया गया था और यह भी एक तथ्य है कि सार्वजनिक बहस के लिए पर्याप्त समय नहीं दिया गया था।

2. "साइबरलॉज़, अपने बहुत ही प्रस्तावना और उद्देश्य में, कहते हैं कि उन्हें ई-कॉमर्स का समर्थन करने के लिए लक्षित किया जाता है, और साइबर ट्रॉट को विनियमित करने के लिए नहीं हैं": - श्री पवन दुग्गल का मानना है कि विधायकों का मुख्य उद्देश्य प्रदान करना रहा है ई-कॉमर्स को विनियमित करने के लिए एक कानून के लिए और उस उद्देश्य के साथ ITAct 2000 पारित किया गया था, जो साइबर अपराध के मामलों से निपटने के लिए इसकी अपर्याप्तता का एक कारण भी है।

इस मौके पर यह कहना पूरी तरह से गलत नहीं होगा कि श्री दुग्गल का उपरोक्त कथन मौलिक रूप से सही नहीं है। इसका कारण यह है कि प्रस्तावना में कहा गया है कि अधिनियम का उद्देश्य ई-कॉमर्स को वैध बनाना है। हालाँकि यह यहीं नहीं रुकती। यह आगे IPC, साक्ष्य अधिनियम, बैंकर की पुस्तक साक्ष्य और RBI अधिनियम में भी संशोधन करता है। इस अधिनियम का उद्देश्य ऐसे सभी मामलों से संबंधित है, जिनमें चिकित्सीय या आकस्मिक उपचार शामिल हैं। यह व्याख्या का एक कार्डिनल नियम है कि "अर्थ को इकट्ठा करने के लिए पाठ को

समग्र रूप से पढ़ा जाना चाहिए"। ऐसा लगता है कि इस कथन की व्याख्या के नियम की कुल अवहेलना की गई है। प्रस्तावना, यदि पूरे के रूप में पढ़ी जाती है, तो यह बहुत स्पष्ट करता है कि अधिनियम समान रूप से ई-कॉमर्स को वैध बनाने और वहां से उत्पन्न होने वाले किसी भी अपराध को रोकने के लिए है।

3. साइबर चड्डी: -साइबर स्टाकिंग साइबर उत्पीड़न, साइबर उपद्रव और साइबर मानहानि सहित हाल के मामलों से पता चला है कि आईटीएक्ट 2000 ने उन अपराधों से निपटा नहीं है। इसके अलावा, यह भी कहा गया है कि भविष्य में साइबर रूप में नए रूप सामने आएंगे, जिन पर ध्यान देने की आवश्यकता है। इसलिए भारत को साइबर अपराध सम्मेलन पर हस्ताक्षर करना चाहिए। हालाँकि दंड प्रक्रिया संहिता के साथ पढ़ा गया ITAct 2000 इन गुंडागर्दी से निपटने में सक्षम है।

4. अधिनियम में साइबर अपराध न तो व्यापक है और न ही व्यापक: -श्री दुग्गल का मानना है कि हमें साइबर अपराध पर समर्पित कानून की आवश्यकता है जो भारतीय दंड संहिता के पूरक हों। समकालीन विचार श्री प्रथमेश पोपट के पास है, जिन्होंने कहा है- "आईटी अधिनियम, 2000 पर्याप्त व्यापक नहीं है और यह 'साइबर अपराध' शब्द को परिभाषित नहीं करता है। श्री दुग्गल ने आगे टिप्पणी की है, "भारत, एक राष्ट्र के रूप में, साइबर अपराध करने वालों को विनियमित करने और उन्हें दंडित करने की तत्काल आवश्यकता है, लेकिन ऐसा करने के लिए कोई विशेष प्रावधान नहीं है। भारतीय दंड संहिता स्कूल के समर्थकों का तर्क है कि IPC समय की कसौटी पर खड़ा है और यह आवश्यक नहीं है कि साइबर अपराध पर कोई विशेष कानून शामिल किया जाए। ऐसा इसलिए है क्योंकि यह उनके द्वारा बहस किया जाता है कि अकेले आईपीसी सभी प्रकार के अपराध के लिए पर्याप्त है। हालांकि, व्यावहारिक रूप से, तर्क में उचित समर्थन नहीं है।यह स्पष्ट रूप से समझा जाना चाहिए कि साइबर अपराध और साइबरस्पेस पूरी तरह से नए घर हैं, जहां नए प्रकार के अपराधों के रूप में दिन में कई नई संभावनाएं और अवसर सामने आते हैं।

5. परिभाषाओं में अस्पष्टता- अधिनियम की धारा 66 में दी गई हैकिंग की परिभाषा बहुत व्यापक है और गलत व्याख्या करने में सक्षम है। इस धारा के गलत होने की पूरी संभावना है और वास्तव में दिल्ली की अदालत ने इसे गलत बताया है। कुख्यात go2nextjob ने यह बहुत स्पष्ट कर दिया है कि उस व्यक्ति का भाग्य क्या हो सकता है जिसे धारा 66 के तहत दर्ज किया गया है या जिसके तहत नेटिज़न्स s तक लगातार खतरे में हैं। 66 अपने वर्तमान रूप में मौजूद है।

आगे की धारा 67 भी कुछ हद तक अस्पष्ट है। शब्द कामुक जानकारी या अश्लील जानकारी को परिभाषित करना मुश्किल है। इसके अलावा बाल भारती मामले से साइबर पोर्नोग्राफी के मामलों से निपटने में हमारी अक्षमता साबित हुई है ।

6. वर्दी कानून: -श्री विनोद कुमार का मानना है कि साइबर चड्डी का मुकाबला करने के लिए दुनिया भर में एक समान साइबर कानून की जरूरत है। साइबर टॉर्ट्स एक वैश्विक घटना है और इसलिए इसे लड़ने की पहल उसी स्तर से होनी चाहिए। उदा। लव बग वायरस के लेखक को उनके देशवासियों ने सराहा।

7. जागरूकता की कमी-एक महत्वपूर्ण कारण यह है कि 2000 का अधिनियम पूरी तरह से सफल नहीं हो रहा है, अपने अधिकारों के बारे में जागरूकता की कमी है। इसके अलावा अधिकांश मामले बिना लाइसेंस के चल रहे हैं। यदि लोग अपने अधिकारों के बारे में सतर्क हैं तो कानून निश्चित रूप से उनके अधिकार की रक्षा करता है। उदा। अक्टूबर 2002 में दिल्ली उच्च न्यायालय ने एक व्यक्ति को नीलामी स्थल पर Microsoft पायरेटेड सॉफ्टवेयर बेचने से रोका। मेट्रोपोलिटन मजिस्ट्रेट दिल्ली की अदालत के समक्ष मामले में उपलब्धि भी दर्ज की गई थी जिसमें एक व्यक्ति को चोरी के क्रेडिट कार्ड का उपयोग करके सोनी के उत्पादों को खरीदने के लिए ऑनलाइन धोखाधड़ी के लिए दोषी ठहराया गया था।

8. अधिकार क्षेत्र के मुद्दे: -साइबर स्पेस के बहुत ही सार्वभौमिक स्वरूप के कारण साइबर अपराध के मामलों में क्षेत्राधिकार भी एक बहस का मुद्दा है। साइबर स्पेस के लगातार बढ़ते हथियारों के साथ क्षेत्रीय अवधारणा लुप्त होती जा रही है। विवाद समाधान के नए तरीकों को पारंपरिक तरीकों के लिए रास्ता देना चाहिए। 2000 का अधिनियम इन मुद्दों पर बहुत मौन है।

9. अतिरिक्त क्षेत्रीय आवेदन: - हालांकि एस .75 इस कानून के अतिरिक्त-क्षेत्रीय संचालन के लिए प्रदान करता है, लेकिन वे तभी सार्थक हो सकते हैं जब प्रावधानों के अनुसार आदेशों का समर्थन किया जाए और सक्षम अधिकारियों द्वारा उनके अधिकार क्षेत्र के बाहर जारी सूचनाओं के लिए वारंट और विनिमय के लिए सहयोग के लिए उपाय किया जाए। सामग्री और कानून प्रवर्तन एजेंसियों के बीच कंप्यूटर अपराधों के सबूत।

10. एक साइबर सेना का निर्माण: -'साइबर आर्मी' शब्द का उपयोग करके मैं आभासी सेना के विचार से अवगत कराना चाहता हूं, बल्कि मैं हाई टेक अपराध के नए रुझानों से निपटने के लिए एक अच्छी तरह से सुसज्जित टास्क फोर्स की आवश्यकता पर जोर दे रहा हूं। सरकार ने सभी महानगरों और अन्य महत्वपूर्ण शहरों में साइबर क्राइम सेल का गठन कर इस दिशा में एक छलांग लगाई है। इसके अलावा केंद्रीय जांच ब्यूरो (CBI) की साइबर अपराध जांच सेल (CCIC) की स्थापना निश्चित रूप से इस दिशा में एक स्वागत योग्य कदम है। ऐसे पुरुष मामले हैं जिनमें सीबीआई को सफलता मिली है। साइबर अपराध के मामलों की वर्तमान स्थिति है -

केस 1: जब एक MNC की महिला ने अश्लील कॉल प्राप्त करना शुरू किया, तो CBI ने पाया कि उसके सहयोगी ने Mumbaidating.com पर अपने व्यक्तिगत विवरण पोस्ट किए थे।

स्थिति:

केस 2 पर जांच : सीबीआई ने यूपी के एक व्यक्ति मोहम्मद फ़िरोज़ को गिरफ्तार किया, जिसने जर्मनी में नौकरी देने वाले विज्ञापन रखे थे। उन्होंने ई-मेल के माध्यम से आवेदकों से बात की और उन्हें दिल्ली में अपने बैंक खाते में पैसा जमा करने के लिए कहा।

स्थिति: चार्जशीट दाखिल नहीं की गई

केस 3: केंद्रीय प्रत्यक्ष कर बोर्ड की आधिकारिक वेबसाइट पिछले साल हैक हो गई थी। चूंकि पाकिस्तान स्थित हैकर जिम्मेदार थे, इसलिए वहां के अधिकारियों को इंटरपोल के माध्यम से सूचित किया गया।

स्थिति: पाक सहयोग नहीं कर रहा है

11. साइबर प्रेमी बेंच: -साइबर सेवी जजों को दिन की जरूरत है। न्यायपालिका दिन के आदेश के अनुसार अधिनियमन को आकार देने में महत्वपूर्ण भूमिका निभाती है। एक ऐसा चरण, जिसे सराहना की आवश्यकता है, वह जनहित याचिका है, जिसे केरेला उच्च न्यायालय ने एक ईमेल के माध्यम से स्वीकार किया है। आज के शब्द में न्यायाधीशों की भूमिका बयान द्वारा एकत्र की जा सकती है- न्यायाधीशों ने 'कानून' को 'कानून बनना चाहिए' पर उकेरा है। विधि आयोग के सदस्य सचिव श्री टी। वीश्वनाथन ने भारत में ई-कोर्ट शुरू करने की आवश्यकताओं पर प्रकाश डाला है। द हिंदू में प्रकाशित अपने लेख में उन्होंने कहा है "यदि शासन का एक क्षेत्र है जहां आईटी भारतीय जनता के लिए एक बड़ा अंतर बना सकता है तो न्यायिक प्रणाली में है"।

12. साइबर अपराध का गतिशील रूप: -साइबर अपराध की गतिशील प्रकृति पर बात करते हुए एफबीआई के निदेशक लुइस फ्रीह ने कहा है, "संक्षेप में, भले ही हमने साइबर घुसपैठ से लड़ने के लिए अपनी क्षमताओं में स्पष्ट रूप से सुधार किया है लेकिन समस्या और

भी तेजी से बढ़ रही है और हम आगे पीछे हो रहे हैं।" मानव मन की रचनात्मकता को किसी भी कानून द्वारा जांचा नहीं जा सकता है। इस प्रकार साइबर अपराध के मामलों के लिए वैधानिक प्रावधानों को लागू करते हुए एकमात्र तरीका उदार निर्माण है।

13. अपराधों की रिपोर्ट करने के लिए हिचकिचाहट:जैसा कि अधिनियम की घातक कमियों में से एक के ऊपर कहा गया है, यह मामले बिना लाइसेंस के चल रहे हैं। एक स्पष्ट कारण गैर-सहकारी पुलिस बल है। यह बात दिल्ली समय चोरी मामले से साबित हुई। "पुलिस आज एक शक्तिशाली बल है जो साइबर अपराध को रोकने में एक महत्वपूर्ण भूमिका निभा सकता है। साथ ही, यह छड़ी को खत्म करने और निर्दोष एस को परेशान करने, उन्हें अपने सामान्य साइबर व्यापार के बारे में जाने से रोक सकता है।" मेरुतुत और बेलगाम में हुई घटना से प्रशासन भी हैरान है। (इन घटनाओं के तथ्यों के लिए naavi.com देखें)। इस अधिनियम के प्रावधानों को पूरी तरह से साकार करने के लिए एक सहयोगी पुलिस बल की आवश्यकता है।

- **निष्कर्ष:**

मानव मन की क्षमता अथाह है। साइबर स्पेस या साइबर स्पेस से साइबर अपराध को खत्म करना संभव नहीं है। उनकी जांच करना काफी संभव है। इतिहास गवाह है कि कोई भी कानून दुनिया से अपराध को पूरी तरह से खत्म करने में सफल नहीं हुआ है। एकमात्र संभव कदम लोगों को उनके अधिकारों और कर्तव्यों (समाज के प्रति सामूहिक कर्तव्य के रूप में अपराध की रिपोर्ट करना) के बारे में जागरूक करना और आगे के कानूनों को एक चेक रखने के लिए और अधिक कठोर बनाना है। निस्संदेह अधिनियम साइबर दुनिया में एक ऐतिहासिक कदम है।हम समर्थक कानून स्कूल के लिए सावधानी के एक शब्द के साथ निष्कर्ष निकालेंगे कि यह ध्यान में रखा जाना चाहिए कि साइबर कानून के प्रावधानों को इतना कठोर नहीं बनाया गया है कि यह उद्योग के विकास को धीमा कर सकता है और प्रति-उत्पादक साबित हो सकता है और एक ही समय में इसके विक्षेपण और आगे के परिणामों पर एक सतर्क जांच रखी जानी चाहिए।

****

ग्रंथ सूची

• पुस्तकें संदर्भित

(1) साइबर अपराध और कॉर्पोरेट दायित्व-क्लूवर-रोहास नागपाल

(2) साइबर कानून की पुस्तिका-मैकमिलन-वकुल शर्मा

(3) साइबर अपराध (कानून) (एक अवलोकन) -विद्या

(4) रामास्वामी अय्यर- टॉर्ट्स-ए लक्ष्मीनाथ और एम श्रीधर का कानून

(5) कानूनी युग- ॥

(6) नागपाल आर। - साइबर अपराध क्या है?

(() समाचार प्रकाशित करें १४.०३.०३

(Her) डेक्कन हेराल्ड १६.०३.०३

(९) हिंदुस्तान टाइम्स ०३.०३.०३

(१०) नागपाल आर- साइबर आतंकवाद को परिभाषित करना

• वेबसाइटें संदर्भित

(१) http://www-bcf.usc.edu/~idjlaw/PDF/13-1/13-1 Rustad Koenig .pdf

(2) http: // www.ebook sdownloadfree.com/Security/Cyber-Situational-A जागरूकता-Issues-and- Research-BI10250.html

(3) en.wikipedia.org/wiki/Cyber कानून

(4) http://www.cyberessays.com/ सूचियाँ / साइबर-टॉर्ट्स / पेज

0. html (5) http://www.slideworld.com/slideshows.aspx/CHAPTER-4-Torts-and-Cyber-Torts-ppt-2225880