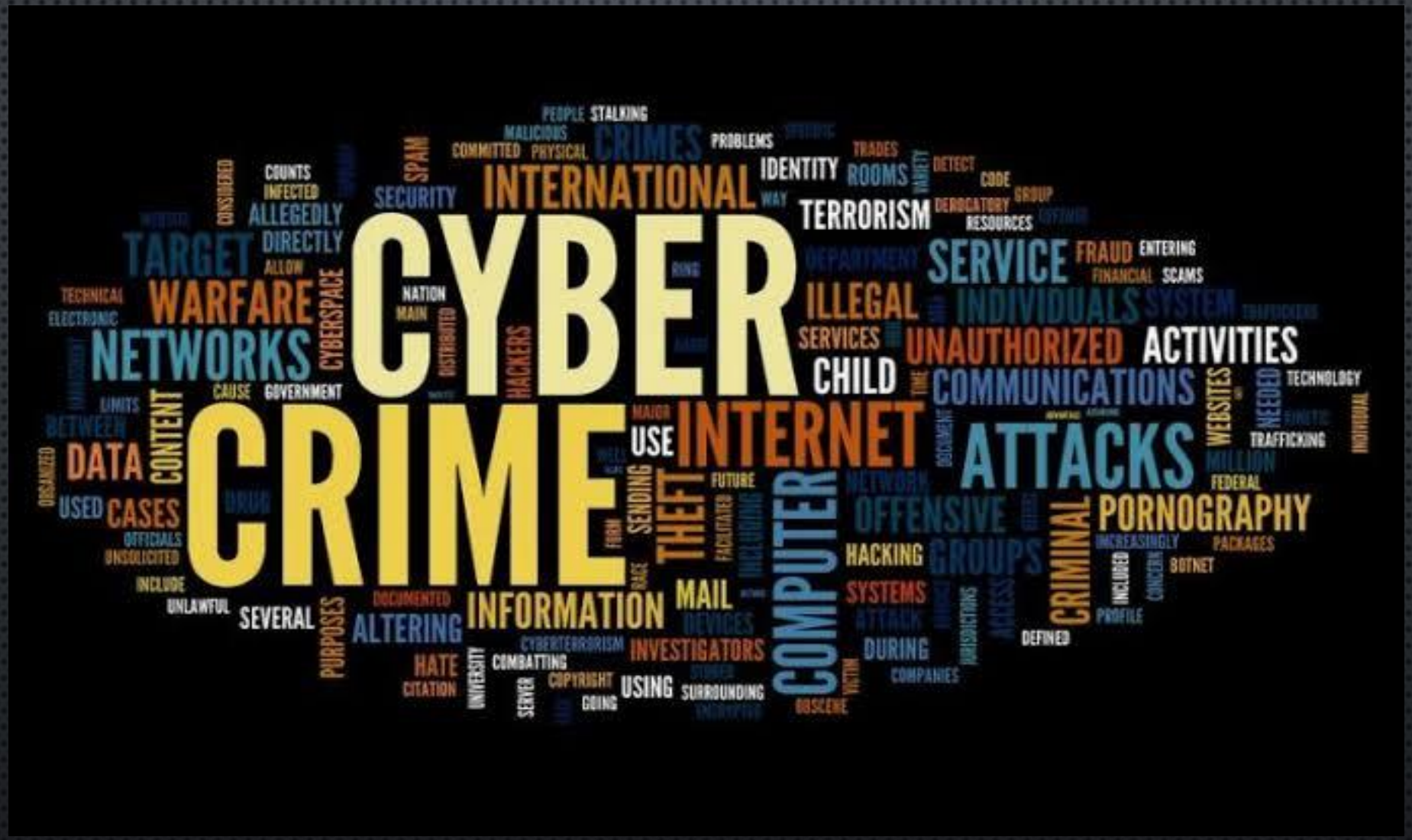

साइबर क्राइम (Cyber Crime)

मनुष्यता के इतिहास के साथ अपराध भी जुड़े रहे हैं। एक सभ्य समाज के साथ-साथ अपराध भी निरंतर बने रहे है। समय और परिस्थितियों के अनुसार अपराधों में भी परिवर्तन होता रहा है। आज वर्तमान समय में साइबर अपराध जैसा शब्द सामने आता है। विश्व के लगभग सभी देशों ने साइबर अपराध से निपटने हेतु कानून बनाए हैं।

प्रौद्योगिकी और इलेक्ट्रॉनिक मीडिया के विकास के बाद कंप्यूटर से संबंधित अपराधों का जन्म हुआ है जिसे आमतौर पर "साइबर अपराध" कहा जाता है।

अपराधों की व्यापक वृद्धि वैश्विक चिंता का विषय बन गई, तथा अपराध एक नई चुनौती के रूप में विश्व भर के सामने आए हैं। यह अपराध अजीब है अपराधी शारीरिक रूप से उपस्थित हुए बिना गुमनाम रूप से और पीड़ित से बहुत दूर रहकर अपराध कर देता है। यह साइबर अपराधी पकड़े जाने के भय के बिना दूर से ही किसी अपराध को कारित कर देते हैं।

इन अपराधों में संचार सेवाओं की चोरी, औद्योगिक जासूसी, साइबर-स्पेस में अश्लील और आपत्तिजनक सामग्री का प्रसार, इलेक्ट्रॉनिक मनी लॉन्ड्रिंग और कर चोरी, इलेक्ट्रॉनिक क्रूरता, आतंकवाद और जबरन वसूली जैसी अवैध कंप्यूटर से संबंधित गतिविधियों की एक विस्तृत श्रृंखला शामिल है। इस ही के साथ इसमे टेली-मार्केटिंग धोखाधड़ी, टेली-संचार का अवैध अवरोधन भी शामिल है।

सायबर अपराध के प्रकार

Types of Cyber Crime

साइबर अपराधों के प्रकारों को जानने के पूर्व इन अपराधों के होने के कारणों को जानना आवश्यक है। विद्वानों की राय और परिस्थितियों के अवलोकन से साइबर अपराध के निम्न कारण प्रतीत होते हैं-

1)- कंप्यूटर में बहुत कम जगह में डेटा स्टोर करने की अनूठी विशेषता है। यह भौतिक या आभासी माध्यम से अधिक आसानी से जानकारी प्राप्त करने और निकालने की सुविधा देता है इसलिए से संबंधित अपराध करना भी आसान होता है।

2)- कंप्यूटर तक पहुंच आसान है और इसलिए, जटिल साइबर स्पेस प्रौद्योगिकी के उपयोग से अनधिकृत पहुंच सुरक्षा प्रणाली को दरकिनार करना आसानी से संभव है।

3)- कंप्यूटर ऑपरेटिंग सिस्टम पर काम करते हैं जो जटिल होते हैं और लाखों कोड से बने होते हैं। साइबर अपराधी इसका सदोष लाभ उठाते हैं

4)- कंप्यूटर प्रणाली की एक महत्वपूर्ण विशेषता यह है कि साक्ष्य कुछ ही समय में नष्ट हो जाते हैं। अपराधियों के लिए अपराध होने के तुरंत बाद सबूतों को नष्ट करना आसान हो जाता है जिससे जांच एजेंसियों के लिए अपराधी पर मुकदमा चलाने के लिए प्रासंगिक सामग्री साक्ष्य एकत्र करना मुश्किल हो जाता है।

5)- कंप्यूटर सिस्टम की सुरक्षा सुनिश्चित करने में कंप्यूटर उपयोगकर्ता की ओर से थोड़ी सी भी लापरवाही के विनाशकारी परिणाम हो सकते हैं क्योंकि साइबर अपराधी अपने आपराधिक लक्ष्य को पूरा करने के लिए कंप्यूटर सिस्टम पर अवैध पहुंच और अनधिकृत नियंत्रण प्राप्त कर सकता है।

.

वायरस (Virus)

वायरस सबसे आम समस्याएं हैं जो कंप्यूटर सिस्टम को गंभीर नुकसान पहुंचा रही हैं। वायरस एक प्रोग्राम या कोड है जो किसी अन्य प्रोग्राम, सेक्टर या दस्तावेज़ को स्वयं को सम्मिलित करके या स्वयं को उस माध्यम से जोड़कर दोहराता है और संक्रमित करता है। वायरस का प्रभाव यह है कि यह डेटा फ़ाइलों और अन्य कार्यक्रमों को नष्ट कर देता है या बदल देता है। दुर्लभ मामलों को छोड़कर, वायरस कंप्यूटर हार्डवेयर को नुकसान नहीं पहुंचाता है। दुनिया भर में वायरस के 5000 से अधिक विभिन्न प्रकार हैं। आमतौर पर वायरस के दो मुख्य वर्ग होते हैं।

फाइल इंफेक्टर्स, जो खुद को साधारण प्रोग्राम फाइलों से जोड़ते हैं। डायरेक्ट- एक्शन वायरस हर बार उस प्रोग्राम को निष्पादित करने के लिए संक्रमित करने के लिए एक या अधिक प्रोग्राम का चयन करता है जिसमें यह शामिल होता है। रेज़िडेंट वायरस स्मृति में कहीं छुप जाता है। पहली बार किसी संक्रमित प्रोग्राम को निष्पादित किया जाता है, और उसके बाद अन्य प्रोग्रामों को निष्पादित होने पर संक्रमित करता है।

वायरस की दूसरी श्रेणी बूट-रिकॉर्ड इंफेक्टर है। ये वायरस संक्रमित करते हैं। डिस्क पर कुछ सिस्टम क्षेत्रों में निष्पादन योग्य कोड पाया जाता है, जो सामान्य नहीं है।

वायरस हॉक्स (Virus Howks)

एक वायरस हॉक्स आम तौर पर एक ई-मेल संदेश प्रकट होता है जो एक विशेष वायरस का वर्णन करता है जो वास्तव में मौजूद नहीं है। ऐसे संदेशों का उद्देश्य कंप्यूटर उपयोगकर्ताओं में दहशत पैदा करना है। लेखक या लेखक चेतावनी को ई-मेल करते हैं और पाठक के लिए इसे दूसरों को अग्रेषित करने के लिए एक अनुरोध शामिल करते हैं। संदेश तब एक श्रृंखला पत्र की तरह फैलता है। जैसे ही लोग इसे प्राप्त करते हैं, पूरे इंटरनेट पर प्रचार-प्रसार करते हैं और फिर इसे फॉरवर्ड करते हैं। यह सलाह हमेशा दी जाती है कि इस तरह के फर्जी वायरस पर कार्रवाई करने के बजाय इसे अनदेखा करें या हटा दें।

वायरस के अलावा, कुछ सामान्य साइबर अपराध हैं जो कंप्यूटर सिस्टम, नेटवर्क या डेटा के खिलाफ निर्देशित होते हैं जबकि अन्य ऐसे भी होते हैं जिनमें कंप्यूटर का उपयोग अपराध करने के लिए एक उपकरण के रूप में किया जाता है।

इसलिए, इस दृष्टिकोण से विचार करने पर, साइबर अपराधों को मोटे तौर पर दो प्रमुख श्रेणियों में वर्गीकृत किया जा सकता है:-

1)- साइबर अपराध जहां कंप्यूटर स्वयं अपराध का लक्ष्य है; तथा

2)- साइबर अपराध जहां कंप्यूटर अपराध का एक उपकरण है। अपराध के लक्ष्य के रूप में कंप्यूटर साइबर अपराध की इस श्रेणी में कंप्यूटर ही अपराध का निशाना बनता है। इन अपराधों में आम तौर पर शामिल हैं:

(1) कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क की तोड़फोड़;

(2) ऑपरेटिंग सिस्टम और कार्यक्रमों की तोड़फोड़;

(3) डेटा/सूचना की चोरी;

(4) बौद्धिक संपदा की चोरी, जैसे कंप्यूटर सॉफ्टवेयर;

(5) विपणन जानकारी की चोरी; तथा

(6) कम्प्यूटरीकृत फाइलों जैसे व्यक्तिगत इतिहास, यौन मामले, वित्तीय डेटा, चिकित्सा जानकारी आदि से प्राप्त जानकारी के आधार पर ब्लैकमेल करना। अपराध को सुविधाजनक बनाने वाले एक उपकरण के रूप में कंप्यूटर अपराध की इस श्रेणी में, कंप्यूटर का उपयोग करने के लिए एक उपकरण के रूप में प्रयोग किया जाता है आतंकवादी और अपराधी दुनिया भर में एन्क्रिप्टेड संदेशों को ई-मेल करने जैसे इंटरनेट तरीकों का उपयोग कर रहे हैं।

इन अपराधों में अपराध को सुगम बनाने के लिए कंप्यूटर प्रोग्रामों में हेराफेरी की जाती है। उदाहरण के लिए, ऑटोमेटेड टेलर मशीन (एटीएम) कार्ड और खातों का कपटपूर्ण उपयोग, ई-बैंकिंग या ई-कॉमर्स से संबंधित धोखाधड़ी, इलेक्ट्रॉनिक डेटा-इंटरचेंज आदि कंप्यूटर का उपयोग करके किए जाते हैं। साइबर पोर्नोग्राफी, सॉफ्टवेयर पायरेसी, ऑनलाइन जुआ, कॉपीराइट उल्लंघन, ट्रेडमार्क उल्लंघन ऐसे अपराधों के कुछ अन्य उदाहरण हैं।

सूचना प्रौद्योगिकी अधिनियम, 2000 (Information Technology Act, 2000)

इंटरनेट और कंप्यूटर से जुड़ी हुई चीजों के लिए भारत में अधिनियमित एक महत्वपूर्ण अधिनियम है। भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 उन सायबर कामों का उल्लेख करते हैं जिन्हें भारत अपराध बनाकर प्रतिबंधित किया गया है। इस आलेख में इनफॉरमेशन टेक्नोलॉजी एक्ट में घोषित किए गए उन सभी अपराधों का उल्लेख किया जा रहा है और उन में किए गए दांडिक प्रावधानों पर चर्चा की जा रही है। विभिन्न अपराध और उनके लिए प्रदान की गई सजा अधिनियम के अध्याय 11 और 11(ए) में निहित हैं। संक्षेप में यह अपराध निम्न है:-

1)- अनधिकृत पहुंच Unauthorized Access (धारा 43):- यह खंड बताता है कि कोई भी व्यक्ति जो कंप्यूटर, कंप्यूटर सिस्टम या कंप्यूटर तक पहुंच प्राप्त करता है और उसे असुरक्षित करता है और यह कार्य उसके द्वारा कंप्यूटर के मालिक या उसके प्रभारी व्यक्ति की अनुमति के बिना किया जाता है तब पीड़ित व्यक्ति को एक करोड़ रुपये से अधिक के मुआवजे के रूप में नुकसान का भुगतान करने के लिए उत्तरदायी होगा।आईटी अधिनियम की धारा 2(1)(ए) में परिभाषित "एक्सेस" शब्द का अर्थ है "कंप्यूटर, कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क के तार्किक, अंकगणितीय या मौद्रिक कार्य संसाधनों में प्रवेश प्राप्त करना, निर्देश देना या संचार करना।" निम्नलिखित कृत्यों को शब्द के दायरे में लाने के लिए माना गया है: अधिनियम द्वारा परिकल्पित "पहुँच":

(1) एक कंप्यूटर पर गैरकानूनी रूप से स्विच करना।

(2) कंप्यूटर पर स्थापित एक सॉफ्टवेयर प्रोग्राम का उपयोग करना।

(3) एक फ्लॉपी डिस्क की सामग्री को अवैध रूप से देखना।

(4) एक कंप्यूटर को अवैध रूप से बंद करना।

(5) अवैध रूप से कंप्यूटर प्रिंट-आउट लेना।

(6) इंटरनेट पर लॉगिंग।

(7) कंप्यूटर को पिंग करना।

अनधिकृत पहुंच का अपराध तब पूरा होता है जब डेटा, डेटा-बेस या जानकारी को एक कंप्यूटर से दूसरे कंप्यूटर में डाउनलोड, कॉपी या अवैध रूप से निकाला जाता है। शब्द "डाउनलोड" एक कंप्यूटर से दूसरे कंप्यूटर में सूचना के हस्तांतरण को दर्शाता है।

2)- सूचना, रिटर्न आदि प्रस्तुत करने में विफलता (धारा 44)
Failure to furnish Information, Returns etc.:-

जहां किसी व्यक्ति को इस अधिनियम या इसके तहत बनाए गए किसी भी नियम के तहत नियंत्रक या प्रमाणन प्राधिकारी को कोई दस्तावेज, रिटर्न या रिपोर्ट प्रस्तुत करने की आवश्यकता होती है, वह उसे प्रस्तुत करने में विफल रहता है, वह प्रत्येक विफलता के लिए 1.5 लाख रुपये से अधिक का जुर्माना देने के लिए उत्तरदायी होगा और चूक के मामले में, प्रतिदिन के लिए 5,000/- रुपये का जुर्माना, जिसके दौरान ऐसी विफलता या चूक जारी रहती है। अधिनियम की धारा 45 अधिनियम के तहत बनाए गए किसी भी नियम के उल्लंघन के लिए दंड का प्रावधान करती है जिसके लिए अधिनियम में विशेष रूप से कोई दंड प्रदान नहीं किया गया है। इस प्रकार, यह धारा अवशिष्ट दंड से संबंधित है और अधिनियम की कुछ धाराओं पर लागू होती है। अधिनियम की धारा 46 उल्लंघनकर्ता को उसके मामले में प्रतिनिधित्व करने का उचित अवसर देने के बाद उस पर लगाए जाने वाले दंड के न्यायनिर्णयन का प्रावधान करती है। न्यायनिर्णयन अधिकारी Adjudicating Officer के पास उन मामलों का न्यायनिर्णयन करने की शक्ति होगी जिनमें चोट या क्षति का दावा पांच करोड़ रुपये से अधिक नहीं है। हालांकि, जहां दावा या क्षति इस सीमा से अधिक है, न्यायनिर्णयन का अधिकार क्षेत्र सक्षम न्यायालय में निहित होगा।

3)- कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़ (धारा 65)
Tampering with Computer Source Documents:-

कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़ को धारा 65 के तहत दंडनीय बनाया गया है। कंप्यूटर स्रोत दस्तावेज़ों (कोड) के संबंध में अपराधों को कानून द्वारा रखा या बनाए रखा जाना है जिसमें जानबूझकर या जानबूझकर

(1) छुपाना
(2) नष्ट करना शामिल है।
(3) परिवर्तन करना।
(4) दूसरे को छुपाना।
(5) दूसरे को नष्ट करना।
(6) दूसरे को कंप्यूटर सोर्स कोड बदलने के लिए प्रेरित करना।

सरल शब्दों में, धारा 65 के प्रयोजन के लिए, छेड़छाड़ का अर्थ है छिपाना (छिपाना या गुप्त रखना)। कंप्यूटर स्रोत दस्तावेज़ को नष्ट करना (ध्वस्त करना या कम करना) या बदलना।

4)- हैकिंग Hacking (धारा 66):-

हैकिंग के आवश्यक तत्व किसी भी व्यक्ति को गैरकानूनी तरीके से गलत तरीके से नुकसान या क्षति पहुंचाने का इरादा है या इस बात का ज्ञान होना कि कंप्यूटर संसाधन दस्तावेज़ में रहने वाली जानकारी को छुपाने, नष्ट करने या बदलने से किसी भी व्यक्ति को नुकसान होगा। इस धारा के तहत यह अपराध तीन साल तक के कारावास या दो लाख रुपये तक के जुर्माने या दोनों से दंडनीय है। पहचान की चोरी हैकिंग का एक सामान्य रूप है जो तेजी से बढ़ता हुआ सायबर अपराध है जो तब होता है जब कोई व्यक्ति किसी धोखाधड़ी को जारी रखने के लिए दूसरे की व्यक्तिगत जानकारी को बिना उसकी जानकारी के विनियोजित करता है।

5)- एक निजी क्षेत्र की छवि को कैप्चर करना(धारा 66 ई):-
Capturing the image of a private area

.

इस धारा में में कहा गया है, "जो कोई भी जानबूझकर या जानबूझकर किसी भी व्यक्ति की गोपनीयता का उल्लंघन करने वाली परिस्थितियों में उसकी सहमति के बिना किसी व्यक्ति के निजी क्षेत्र की छवि को कैप्चर, प्रकाशित या प्रसारित करता है, उसे कारावास से दंडित किया जाएगा, जिसे तीन साल तक बढ़ाया जा सकता है या 2 लाख रुपये से अधिक के जुर्माने या दोनों के साथ। सूचना प्रौद्योगिकी गोपनीयता को सक्षम करने वाला कानून नहीं है, इसलिए निगरानी में गोपनीयता की चुनौतियों का इसमें पूरी तरह से समाधान नहीं किया गया है। हालांकि, विशेषज्ञों का मानना है कि सीसीटीवी कैमरों को नियंत्रित करने वाले कानून अधिक व्यापक होने चाहिए और यह केवल दृश्यता तक सीमित नहीं होना चाहिए। अधिनियम की धारा 66 में धारा 66ए से 66एफ जोड़ी गई। इसमे अधिनियम सजा निर्धारित करता है अश्लील संदेश भेजने, पहचान की चोरी, धोखा देने जैसे अपराधों के लिए कंप्यूटर संसाधनों का उपयोग कर प्रतिरूपण, इंटरनेट सुरक्षा का उल्लंघन शामिल है।

6)- इलेक्ट्रॉनिक रूप में अश्लील सूचना का प्रकाशन (धारा 67):-
Publication of obscene information in electronic form

इंटरनेट पर अश्लीलता सूचना प्रौद्योगिकी अधिनियम की धारा 67 के तहत दंडनीय कार्य है। शब्द "इस खंड के उद्देश्य के लिए प्रकाशित करने का अर्थ है, "आम तौर पर ज्ञात करना, औपचारिक रूप से प्रचार करना या सार्वजनिक रूप से बिक्री के लिए प्रतियां जारी करना।" वेबसाइट पर अश्लील सामग्री का प्रसार एक अपराध है जिसमें तीन साल तक की कैद या जुर्माना हो सकता है। जो दो लाख रुपये तक या दोनों के साथ हो सकता है। पीडोफाइल आमतौर पर अश्लील सामग्री वितरित करके किशोरों को लुभाते हैं, फिर वे उनसे सेक्स के लिए मिलने की कोशिश करते हैं और यौन गतिविधियों में उनकी नग्न तस्वीरें लेते हैं और इस तरह उन्हें ब्लैकमेल करते हैं और इस ही से उन्हें यौन शोषण के लिए मजबूर करते हैं।

7)- नियंत्रक के निर्देशों का पालन करने में विफलता (धारा 68)
Failure to comply with the instructions of the Controller

धारा 68 नियंत्रक या प्रमाणन प्राधिकरण को किसी भी कंप्यूटर संसाधन के माध्यम से प्रेषित किसी भी जानकारी को इंटरसेप्ट करने के लिए अधिकृत करता है, जब भी ऐसा करना समीचीन हो। इस तरह के आदेश का पालन करने में विफल रहने पर व्यक्ति को तीन साल तक की कैद या दो लाख रुपये तक का जुर्माना या दोनों हो सकता है। तथापि, नियंत्रक या प्रमाणन प्राधिकारी द्वारा पारित आदेश किया जाना चाहिए यदि आईटी के किसी भी प्रावधान का अनुपालन सुनिश्चित करना आवश्यक हो।

8)- कंप्यूटर संसाधन के माध्यम से किसी सूचना के अवरोधन/निगरानी/डिक्रिप्शन के निर्देश जारी करने की शक्ति (धारा 69):-

नियंत्रक या प्रमाणन प्राधिकारी या ऐसे प्राधिकरण का कोई कर्मचारी अधिकृत है। किसी भी कंप्यूटर संसाधन के माध्यम से प्रेषित किसी भी जानकारी को इंटरसेप्ट करने के लिए जब भारत की संप्रभुता या अखंडता, राज्य की सुरक्षा, विदेशी राज्यों के साथ मैत्रीपूर्ण संबंधों या सार्वजनिक व्यवस्था के हित में या किसी संज्ञेय अपराध को करने के लिए उकसाने को रोकने के लिए ऐसा करना समीचीन है। 2008 के संशोधन अधिनियम द्वारा मूल अधिनियम में डाली गई नई धारा 69-ए केंद्र सरकार को भारत की संप्रभुता और अखंडता के हित में, किसी भी कंप्यूटर संसाधन के माध्यम से किसी भी जानकारी की सार्वजनिक पहुंच को अवरुद्ध करने के लिए निर्देश जारी करने का अधिकार देती है। हालाँकि, ऐसा करने के कारणों को उन्होंने लिखित रूप में दर्ज किया। मध्यस्थ जो इस धारा के तहत सरकार द्वारा जारी निर्देशों का पालन करने में विफल रहता है, उसे एक वर्ष की अवधि के लिए कारावास से दंडित किया जाएगा, जिसे सात साल तक बढ़ाया जा सकता है, और जुर्माना भी लगाया जा सकता है। 2008 के आईटी (संशोधन) अधिनियम द्वारा सम्मिलित की गई धारा 69-बी सरकार को साइबर सुरक्षा उद्देश्यों के लिए किसी भी कंप्यूटर संसाधन के माध्यम से ट्रैफिक डेटा या सूचना की निगरानी और संग्रह को अधिकृत करने का अधिकार देती है। मध्यस्थ द्वारा इस प्रावधान के उल्लंघन की सजा तीन साल तक की कैद और जुर्माना भी हो सकता है। इस खंड में संदर्भित जानकारी ई-मेल संदेशों पर लागू होगी।

9)- प्रोटेक्टेड सिस्टम तक पहुंच (धारा 70):-
Access to Protected System

धारा 70 में निहित विशेष प्रावधान संरक्षित सिस्टम से संबंधित हैं। यह खंड प्रदान करता है
में अधिसूचना द्वारा, कभी भी घोषित कर सकती है कंप्यूटर, कंप्यूटर सिस्टम या कंप्यूटर नेटवर्क ए
व्यक्ति जो पहुंच सुरक्षित करता है या किसी संरक्षित तक पहुंच सुरक्षित करने का प्रयास करता है। इ
भी प्रकार के कारावास के साथ सजा जो दस साल तक बढ़ाई जा सकती है और जुर्माने के लिए भी
और 70-बी को सूचना प्रौद्योगिकी अधिनियम द्वारा मूल अधिनियम में सम्मिलित किया गया
राष्ट्रीय नोडल एजेंसी की नियुक्ति का प्रावधान करता है जो केंद्रीय सूचना अवसंरचना के संरक्षण
सभी उपायों के लिए जिम्मेदार होगी। सरकार का कोई भी संगठन। इस उद्देश्य के लिए राष्ट्रीय
सकता है। इस प्रकार नियुक्त राष्ट्रीय नोडल एजेंसी को भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल