Inspira- Journal of Modern Management & Entrepreneurship (JMME)
ISSN : 2231–167X, GIF: 2.7282, CIF: 5.647, Volume 10, No. 01, January, 2020, pp. 262-272

साइबर अपराध और निजता का अधिकारः प्रभाव तथा प्रौद्योगिकी अधिनियम 2000
(CYBER CRIMES& RIGHT TO PRIVACY IFFECT & IT ACT 2000)

डॉ. सीमा शर्मा*

परिचय

भारत में विगत सदी के आठवें दशक में हुए सूचना प्रौद्योगिकी तथा इलेक्ट्रानिक मीडिया के विकास के परिणामस्वरूप कम्प्यूटर जनित अपराधों का नया वर्ग अस्तित्व में आया है जिसे साइबर अपराध के नाम से जाना जाता है। साइबर अपराधों की सबसे बड़ी विशेषता है कि यह अपराधी की घटनास्थल पर उपस्थिति के बिना किसी भी स्थान पर कारित हो सकते हैं तथा अपराधी व उसके अपराध का शिकार हुआ पीड़ित व्यक्ति एक–दुसरे से पूर्णतः अनजान रहते है। इन अपराधों की एक अन्य विशेषता यह भी है कि इसे कारित करने वाला अपराधी स्वयं अदृश्य रहते हुए कम्प्यूटर तकनीक के माध्यम से लक्षित व्यक्ति (Victim-Target) को क्षति कारित करता हैं, अतः उसके पकड़े जाने की संभावना प्रायः नहीं के बराबर रहती है।

साइबर अपराध की परिभाषा

सूचना प्रौद्योगिकी अधिनियम, 2000 के अन्तर्गत साइबर अपराध को परिभाषित नहीं किया गया है। अनेक विद्वानों का मत है कि इसकी परिभाषा अन्य परंपरागत अपराधों की परिभाषा से मूलतः भिन्न नहीं है क्योंकि अन्य अपराधों की भॉति साइबर अपराध में भी कोई ऐसा कार्य करना या कार्यलोप जिससे विधि का उल्लघंन होता है राज्य द्वारा दंडनीय होगा। साइबर अपराध एक ऐसी अवैध गतिविधि है जिसमें कम्प्यूटर को एक माध्यम के रूप में या निशाने (Target) के रूप में या अपराध करने के माध्यम के रूप में प्रयुक्त किया जाता है। दूसरे शब्दों में, साइबर अपराध एक ऐसा अवैधानिक कृत्य है जिसमें कम्प्यूटर साधन के रूप में या साध्य (लक्ष्य) के रूप में प्रयूक्त होता है।

साइबर अपराध की प्रकृति

वास्तव में देख जाए तो अपराध अन्तर्देशीय स्वरूप का होता है क्योंकि इसका प्रभाव विश्व के विभिन्न देशों तक होता है। विभिन्न देशों के निहीत हित ही साइबर विरोधी अन्तर्राष्ट्रीय विधायन के लिए बाधक सिद्ध हुए है। देशों के राष्ट्रीय एवं अन्तर्राष्ट्रीय हितों में टकराव के कारण इस सम्बन्ध में कोई सर्वमान्य कानून पारित नहीं हो सका है जिसके कारण साइबर अपराधों में दिनोंदिन वृद्धि हो रही है। साइबर अपराध का रूवरूप ही कुछ ऐसा है कि इसमें अपराधकर्ता दूर रहकर भी अपने अपराध के लक्ष्य बिन्दु के सर्म्पक या सामने आए बिना अपने अपराध को क्रियान्वित कर सकता है। जिसके कारण उसके पकड़े जाने के अवसर नगण्य प्राय होते है और यदि पकड़ा भी जाये तो इसे साक्ष्य के आधार पर साबित करना अत्यन्त कठिन होता है।

साइबर अपराध में तीव्रगति से वृद्धि के कारण

साइबर अपराधों के विभिन्न तरीकों का उल्लेख करने के पूर्व यह जान लेना आवश्यक है कि इन अपराधों में अन्य रूढ़िगत अपराधों की तुलना में शीघ्रता से वृद्धि के क्या प्रमुख कारण है तथा साइबर अपराधी सूचना प्रौघोगिकी का दुरूपयोग करने की ओर क्यो प्रवृत्त हो रहे हैं? कम्प्यूटर अपराधों की बहुकला के मुख्य कारण निम्नलिखित हैं–

* पीडीएफ शोधार्थी, राजनीति विज्ञान विभाग, राजस्थान विश्वविद्यालय, जयपुर राजस्थान।

- कम्प्यूटर में थोड़ी सी जगह में वृहद डॉटा संग्रहीत रखने की विलक्षण क्षमता होने के कारण इसमें विविध सूचनाएँ एकत्रित कर संजोकर रखी जा सकती हैं जिसका किसी भी समय आवश्यकतानुसार उपयोग किया जा सकता है। इसी प्रकार आवश्यकता न रहने पर जानकारी को सरलता से हटाया (deleted) भी जा सकता है।
- सुरक्षा उपायों की अनदेखी करते हुए कम्प्यूटर में अनधिकृत अभिगमन (न्दंनजीवतपेमकंबबमे) द्वारा गोपनीय या अवांछित व्यक्तिगत जानकारी हासील करना अपेक्षाकृत सरल होता है।
- कम्प्यूटर एक जटिल आपरेटिंग सिस्टम (Operating System) से चलित होता है जिसमें हजारों कूट–संकेत (Codes) रहते है। साइबर अपराधी मानव–मस्तिष्क की विस्मृति (Falliability of human mind) का नाजायज फायदा उठाते हुए कम्प्यूटर सिस्टम में अवैध प्रवेशन द्वार संचयित जानकारी चुरा लेते है तांकि उससे व्यक्ति को ब्लैकमेल किया जा सके।
- कम्प्यूटर सिस्टम का एक मुख्य लक्षण यह है कि इसमें से सबूत को आसानी से नष्ट किया जा सकता है। अतः आपराधित्व लक्ष्य साध्य होते ही साइबर अपराधी सर्वप्रथम अपने विरूद्ध सबूतों को नष्ट कर देता है ताकि वह अन्वेषण संस्थाओं की पकड़ के बाहर रहे और उसके विरूद्ध अभियोजन का कोई साक्ष्य उपलब्ध न रहे।
- कम्प्यूटर–प्रयोक्ता (computer user) द्वारा कम्प्यूटर में एकत्रित करके रखी गई जानकारी को सुरक्षित रखने में तनिक भी असावधानी उसे घोर क्षति करित कर सकती है क्योंकि साइबर अपराधी कम्प्यूटर सिस्टम में से अनधिकृत अभिगमन (unauthorised accesss) द्वारा जानाकरी चुराकर उसका दुरूपयोग कर सकता है।

वायरस (Viruses)

वर्तमान कम्प्यूटर वायरसों के कारण कम्प्यूटर को गम्भीर क्षति कारित हो रही है। यहॉ 'वायरस' से आशय कोई फैलने वाली चिकित्सीय बिमारी न होकर ऐसे कम्प्यूटर प्रोग्राम या कूट–संकेत (Program or Code) जो किसी अन्य प्रोग्रामों में प्रवेश कर उन्हें प्रतिकृत (replicate) कर देता है और इस प्रकार कम्प्यूटर में संगृहीत प्रोग्राम दूषित या विनष्ट हो जाता है। इससे डाटा फाइलों को भी क्षति कारित होती है। वर्तमान में विश्व में लगभग 5000 से अधिक वायरस की दशाएँ (Strains of virus) विद्यमान है। उदाहरणार्थ, लव–बग (Love-Bug) वाइरस के कारण मई, 2000 में विश्व की अनेक इन्टरनेट साइट्स को गम्भीर क्षति कारित की। इसी प्रकार हाल ही में पाकिस्तान द्वारा विकसित कम्प्यूटर वेबसाइट को विकृत कर दिया।

सामान्यतः वायरस के दो मुख्य प्रकार है जिन्हे (1) फाइल इन्फेक्टर्स तथा (2) बूट–रिकार्ड इन्फेक्टर्स कहा जाता है।

फाइल इन्फेक्टर्स सीधे मारक (direct action) हो सकते है या निवासी (Resident) सीधे मार करने वाले फाइल इन्फेक्टर्स एक ही समय या अधिक प्रोग्रामों को विदूषित करते है जबकि निवासी (resident) वायरस कम्प्यूटर की मेमोरी में छिपा रहता है और जब भी किसी प्रोग्राम का निष्पादन किया जाता है, वह उसे संक्रमित कर देता है।

बूट रिकार्ड वायरस इन्फेक्टर्स निष्पादनीय कूट–संकेत (executable code) को संक्रमित करता है जो कि कम्प्यूटर डिस्क (disk) के सिस्टम–भाग में पाया जाता है। उदाहरणार्थ, ब्रेन (Brain), अझुसा (Azus) माइकेलांगेलो (Michelangelo), सोन्डे (Sonde) आदि बूट रिकार्ड वायरस

सामान्य वर्गीकरण (General Classification)

साइबर अपराधों के सामान्य तथा सरलीकृत वर्गीकरण के अन्तर्गत इन अपराधों को तीना वर्गो में विभक्त किया गया है, जो निम्नानुसार है–

- **व्यक्ति विशेष के विरूद्ध साइबर अपराध –** इसमें ई–मेल में हेराफेरी करके व्यक्ति को संत्रास पहुॅचाया, मानहानि, कम्प्यूटर सिस्टम या प्रोग्राम में अनधिकृत अभिगमन (unauthorised access), अभद्र या अश्लील अंग प्रदर्शन (indecent exposures), छल, वेबसाइट पर अश्लील साहित्य का प्रदर्शन आदि शामिल हैः
- **संपत्ति के विरूद्ध साइबर अपराध** –कम्प्यूटर को जानबुझकर क्षतिग्रस्त करना, उसमें वायरस संक्रमित करना, सेवा उपलब्धि को रोकना (denial of service attack)ः बौद्धिक संपदा अधिकारों का हनन, इन्टरनेट टाइम–चोरी (time theft), प्रतिबंधित वस्तुओं का क्रय–विक्रय आदि का समावेश है।
- **समाज या राज्य के विरूद्ध साइबर अपराध** – इसमें साइबर आतंकवाद, वित्तीय घोटाले, कपट, ऑनलाइन जुआ, अश्लीलता आदि सम्मिलित है।

कम्प्यूटर सिस्टम के माध्यम से साइबर अन्तरिक्ष में कारित होने वाले साइबर अपराध (Cyber crimes committed in Cyber Space through Computer Systems)

ऐसे अनेक साइबर अपराध है जो कम्प्यूटर सिस्टम के माध्यम से साइबर अन्तरिक्ष में घटित होते है। इनमें निम्नलिखित अपराध विशेष उपलब्ध है–

स्टेकिंग (Stalking)

अधिकांशतः पुरूष साइबर अपराधी किसी महिला को लक्षित कर उसके ई–मेल पते पर अनचाहे भदे तथा अश्लील सन्देश भेजकर स्टेकिंग (stalikng) करते हैं। वह अपना अपराध कम्प्यूटर के माध्यम से घर बैठकर ही कर सकते है तथा उसे पकड़े जाने का भय नहीं रहता क्योंकि भौतिक रूप से उसकी कहीं उपस्थिति नहीं रहने के कारण इसकी पहचान नहीं की जा सकती है और साइबर स्पेस में अपराध घटित होने के कारण अपराधी द्रश्यमान भी नहीं होता है।

अधिकांशतः महिलाऍ तथा किशोर वयस्क ही स्टेकिंग के शिकार होते है क्योंकि अपराधी इन्हें ही अपराध का लक्ष्य बनाते है। इस अपराध के लिए भा. द. स. में तीन वर्ष के कारावास का प्रावधान है तथा पुनः अपराध किया जाने पर पॉच वर्ष के कारावास का दण्ड देय है। पीड़िता स्टेकर के विरूद्ध न्यायालय से व्यादेश (injunction) की मॉग कर सकती है।

इस अपराध के तेजी से फैलने के अनुमान इसी बात से लगाया जा सकता है कि सन् 2013 में इसे दण्ड विधि के अन्तर्गत घोषित किया जाते है प्रथम नौ माह में अकेले दिल्ली में 916 प्रकरण पुलिस द्वारा दर्ज किये गए। स्टेकिंग के अपराध के विषय में दिल्ली की वरिष्ठ अधिवक्ता पिंकी आनन्द का मानना है कि यदि इस अपराध का पता लगते ही इसे न रोका जाए, तो महिलाओं के प्रति जघन्य अपराध होने की आशंका सदैव बनी रहेगी जिसे अपराधशास्त्र की भाषा में 'टूटी खिड़की का सिद्धान्त' (Broken Window Therory) कहा गया है। इस सिद्धान्त के अनुसार जो व्यक्ति खिड़की तोड़ने के लिए पत्थर फेंकते हैं, वे बड़े अपराध करने की और प्रवृत्त हो सकते हैं,

कैलोफोर्निया विश्व में ऐसा देश था जिसने स्टेंकिग को सर्वप्रथम अपराध के रूप में दण्ड विधि में शामिल किया। अब सभी अमरीकी राज्य इसे अपराध घोषित कर चुके है। कनाडा में इस अपराध के लिए दस वर्ष के कारावास का दण्ड निर्धारित है।

स्टेकिंग के अपराध का शिकार होने के बचने के उपाय

इस अपराध के प्रति विशेषकर महिलाओं को सतर्क करते हुए उन्हे इसका शिकार होने से बचने के लिए निम्नलिखित सावधानियॉ बरतनी चाहिए–

- स्टेंकिग करने वाली अपराधी से सीधा सम्पर्क करने से बचें क्योंकि सम्पर्क करने से वह पीड़िता को और अधिक सन्त्रास पहुॅचा सकता हैः

- बिना किसी भया या संकोच के इसकी रिपोर्ट तत्काल पुलिस में करेः
- ई–मेल या कम्प्यूटर द्वारा स्टेकर द्वारा भेजे गए सन्देश, टेवस्ट या इलेक्ट्रानिक पत्र आदि साक्ष्य हेतु सम्भाल कर रखेः
- आपात फोन नम्बरों को अपने पास तत्काल उपलब्ध रखें ताकि अविलम्ब कार्यवाही की जा सकेः
- भले ही कोई आसन्न संकट (immedicate danger) प्रतीत न हो, फिर भी थोड़ी भी असहजता होने पर सहायता की मॉग करने में संकोच न करेः
- अकेली यात्रा करते समय सूने स्थान, सड़कों, गलियों आदि को टालें।

हेकिंग (Hacking)

वर्तमान समय में हेकिंग सर्वाधिक घटित होने वाला साइबर अपराध है। हेकिंग के अनेक प्रकार है जैसे, वेब स्पूफिंग (Web-spoofing), ई–मेल बांबिग (E-mail Bombing), ट्रोजन हमले (Trojan Attacks), वायरस हमले (Virus Attacks), पासवर्ड क्रेकिंग (Password Cracking) आदि। सरल शब्दों में हेकिंग से आशय है कम्प्यूटर नेटवर्क के माध्यम से अनाधिकृत–अभिगमन (unauthorised access) का प्रयास करते हुए संकलित डाटा या प्रोग्राम को नष्ट करना या उससे अनधिकृत छेडछाड़ करना।

ट्रोजन हमला (Trojan Attack) एक ऐसा अनाधिकृत प्रोग्राम है जो किसी अन्य की कम्प्यूटर सिस्टम पर स्वयंः को एक अधिकृत प्रोग्राम दर्शाते हए, नियन्त्रण प्राप्त कर लेता है।

पासवर्ड तथा युजर नेम, दोनों ही वेबसाइट धारक के पास गोपनीय रहते है। यदि किसीतहर हेकर को उत्पीड़ित व्यक्ति का पासवर्ड या यूजरनेम का पता लग जाए, तो वह स्वयं वेबसाइट धारक के रूप में डाटा या फाइल में हेरफेर, जोड़तोड़ या दुरूपयोग कर सकता है। यदि हेकर चाहे तो पूरी वाणिज्यिक वेबसाइट या ई–मेल सिस्टम को तहस–नहस करके पुरे व्यापार का ही सर्वनाश कर सकता है।

ई–मेल स्पूफिंग (E-mail spoofing)

एक स्पूफिंग (spoofing) किया गया ई–मेल उसे कहते है जो मूल ई–मेल का दुर्व्यपदेशन (गलत–बयानी) करता है। अर्थात उसके मूल–पाठ (original text) को चालाकी से परिवर्तित कर दिया जाता है। उदाहरणार्थ यदि 'अ' किसी को धमकी भरा ई–मेल स्वयं के नाम के बजाय 'ब' के नाम से करता है, जो कि ई–मेल प्राप्तकर्ता का मित्र है, तो इसे 'अ' द्वारा किसी गया ई–मेल स्पूफिंग कहा जायेगा।

साइबर आतंकवाद (Cyber Terrorism)

प्रायः सभी देशों द्वारा कड़े सीमा सुरक्षा उपाय किये जाने पर भी उन्हे आतंकवाद की समस्या से जुझना पड़ता है। नई आधुनिकतम संचार–तकनीकों के विकसित होले के फलस्वरूप रूढ़िगत आतंकवाद के तरीकों में गहन परिवर्तन हुआ है और अब कम्प्यूटर और इन्टरनेट की सहायता से सुदुर देशों से ही आतंकवादी हमले संयोजित किया जाना संभव है।

अमेरिका के राष्ट्रीय अधोसरंचना सुरक्षा केन्द्र (Us National Infra-struture Protection Center) ने साइबर आतंकवाद को परिभाषित करते हुए कहा है कि यह एक ऐसा अपराधिक कृत्य है जो कम्प्यूटर तथा दुर संचार माध्यमों से कारित किया जाता है जिसका परिणाम जघन्य हिंसा तथा लोक सेवाओं को अस्त–व्यस्त या ध्वस्त (distruction or disruption) होने के रूप में होता हैं साइबर आतंकवाद को क्रियान्वित करने के दो प्रमुख तरीके अपनाए जाते हैः– (1) इन्टरनेट के दुरूपयोग द्वारा या (2) साइबर हमले द्वारा नाजुक अधोंसरंचना (Critical infa-struture) को ध्वस्त या विनष्ट करके।

साइबर आतंकवाद के दुष्परिणाम किसी देश के लिए घरेलु (domestic) तथा अन्तर्राष्ट्रीय स्वरूप के हो सकते है। साइबर आतंकवादी वह व्यक्ति होता है जो निम्नलिखित में से किसी उदेश्य की पूर्ति हेतु कम्प्यूटर सिस्टम का उपयोग करता है–

- जनता या जनता के किसी वर्ग या समुदाय में दहशत का वातावरण फैलाना, या
- विभिन्न धर्मावलंबियों, जातियों, भाषियों या सामूदायिक संगठनों में उन्माद फैलाना तथा इनमें वैमनस्य या आपसी घृणा पैदा करनाः या
- विधि द्वारा स्थापित सरकार को आतंकित करना या डराना–धमकानाः या
- किसी राष्ट्र की अखंडता या संप्रभुत्ता (integrity or sovereignty) को संकट उत्पन्न करना, या

उपर्युक्त से कम्प्यूटर नेटवर्क के माध्यम से कारित कोई भी कृत्य साइबर आतंकवाद का अपराध माना जाएगा। विश्व में तेजी से फैलते हुए साइबर आतंकवाद के निवारण हेतु राष्ट्रसंघ ने अपने सदस्यों को सचेत करते हुये कहा है कि उन्हे अपनी साइबर फोरेन्सिक व्यवस्था को अधिक कारगर और मजबूर बनानी चाहिए तथा अन्य राष्ट्रों से सहयोग करना चाहिए।

साइबर अश्लील–लेखन (Cyber Pornography)

वेबसाइट एवं इन्टरनेट पर अश्लील सन्देश तथा प्रतिबंधित साहित्य दर्शाए जाना एक गम्भीर अपराध है क्योंकि ऐसे अश्लील साहित्य से बच्चों तथा किशोर वयस्कों के मस्तिष्क पर बुरा प्रभाव पड़ता है। यह साहित्य सामग्री या सन्देश इलेक्ट्रानिक फार्म में कम्प्यूटर पर उपलब्ध कराई जाती हैं ताकि युवा वर्ग इनकी और आकर्षित हो और अनैतिक लैगिंक व्यापार को बढ़ावा

साइबर मानहानि (Cyber Defamation)

साइबर मानहानि, परंपरागत मानहानि के अपराध से केवल इस अर्थ में भिन्न है कि उसमें किसी व्यक्ति की मानहानि के लिए साइबर अन्तरिक्ष को माध्यम के रूप में अपनाया जाता है। कोई ऐसा अपमानजनक कथन वेबसाइट या ई–मेल द्वारा लक्षित व्यक्ति भेजा जाना जिससे उसकी प्रतिष्ठा को ठेस पहुॅचे साइबर मानहानि का अपराध होगा।

मनी लाउड्रिंग (Money Laundering)

इस साइबर अपराध में परिवहमान धनराशि (Money in Transit) को बीच में ही अवैध रूप से डाउनलोड कर लिया जाता है। इस अपराध द्वारा इन्टरनेट के माध्यम से काले धन को सफेद धन में परिवर्तित किया जाता है। ताकि अपराधी काले धन की कमाई के आरोप से स्वयं को बचा सके। इस अपराध की गम्भीरता का अनुमान इस बात सक ही लगाया जा सकता है कि सन् 2005 में प्रवर्तन निर्देशालय द्वारा मनी लाउड्रिंग के 146 प्रकरणों में की गई जब्ती (मप्रनतमे) में लगभग 10 करोड़ रूपये का काला धन उजागर हुआ। सन् 2014 में पश्चिम बंगाल के सारधा घोटाले (Saradha Scam) में अपराधियों ने मनी लाउड्रिंग द्वारा सामान्य जनों के कई करोड़ रूपये डकार लिये और इन लोगो को अपने मेहनत से कमाए हुए धन से वन्चित होना पड़ा। उल्लेखनीय है कि अनेक ऐसे प्रकरण भी है जिनमें कोई व्यक्ति पीड़ित के रूप में नहीं है फिर भी घोटाले में करोड़ो रूपयों की मनी लाउड्रिंग हुआ है, जैसे कोलगेट घोटाला (कोयले की 245 खदानो का अवैध आवण्टन) 2–जी स्पेक्ट्रम घोटाला आदि।

डाटा डिडलिंग (Data Diddling)

इस अपराध में कम्प्यूटर में उपलब्ध डाटा को सुक्ष्म तरीके से बदल दिया जाता है या मिटा दिया जाता है ताकि उसे पुनः अपने मुल रूप में न लाया जा सके और इस तरह उसकी परिशुद्धता (ccuracy) समाप्त हो जाए। इस अपराध में कम्प्यूटर में डाटा डाले जाने के पूर्व या डाटा डाले जाते समय इसे बदल दिया जाता है जिससे कि सत्यता प्रभावित होती है।

साइबर अपराधों के निवारण हेतु विधिक उपाय (Legal Measures For Prevention of Cyber Crimes)

विधि का मुख्य प्रयोजन समाज की आवश्यकताओं की पूर्ति करना तथा शांति व्यवस्था बनाए रखना है। सामाजिक परिवर्तनों करना आवश्यक होता है। इसी श्रृंखला में सूचना प्रौद्योगिकी एवं कम्प्यूटर विज्ञान की प्रगति

के फलस्वरूप इनसे जुड़े अपराधों की रोकथाम के लिए कानून निर्मित किये जाना तथा विद्यमान कानूनों में संशोधन किया जाना आवश्यक हूआ। वर्तमान 21 सदी के कम्प्यूटर–युग में अनेक ऐसे नये अपराध अस्तित्व में आये जिनके बारे में पहले कभी कल्पना भी नहीं की जा सकती थी। अब साइबर अपराध एक ही स्थान से दुरस्थ देशो में विभिन्न जगहो पर कारित होना सम्भव हो गया हैं जबकि अपराधी का अपराध के स्थान पर उपस्थित रहना आवश्यक नहीं है।

इनसे कम्प्यूटर नेटवर्क के माध्यम से डाटा की चोरी, अश्लील सामग्री का प्रसारण, अनधिकृत–अभिगमन (unauthorised access or Hacking), वाणिज्यिक एवं बैंको में धोखाधड़ी, गबन आदि के साइबर अपराध बहुलता से घटित हो रहे है। चूंकि साइबर अन्तरिक्ष की कोई भौगोलिक सीमाएँ नहीं होती और न इसमें लिंग, आयु, स्वाभाव आदि जैसे मानवीय लक्षण ही होते है।

सूचना प्रौद्योगिकी अधिनियम, 2000

भारतीय दण्ड संहिता के प्रावधानों के प्रयोज्यता (Applicability of the provision of IPC) की परिधि को विस्तृत करने के लिए सूचना प्रौद्योगिकी अधिनियम द्वारा इसमें नई धारा 29–। जोड़ी गई ताकि जहॉ कहीं भी दस्तावेजो (Documents) से सम्बन्धी अपराध का उल्लेख है उसमे 'इलेक्ट्रानिक दस्तावेजो' को भी शामिल माना जाए। यह नई धारा इस प्रकार है–

- लोक सेवक, जो क्षति कारित करने के आशय से अशुद्ध दस्तावेज रचता है (धारा 167 भा. दं. सं.)
- समनों की तमील या अन्य कार्यवाही से बचने के लिए करार हो जाना (धारा 172)
- समन की तामील का या अन्य कार्यवाही का या उसके प्रकाशन को रोकना या निवारण करना (धारा 173)
- दस्तावेज पेश करने के लिए वैध रूप से आबद्ध व्यक्ति का लोक सेवक को दस्तावेज पेश करने में लोप (omission)। (धारा 175)
- साक्ष्य के रूप में किसी दस्तावेज को पेश किये जाने से रोकने के लिए उसको नष्ट करना (धारा 204)
- अश्लील पुस्तकों आदि का विक्रय (धारा 292)
- कूटरचना (forgery)। (धारा 463)
- रिष्टि (mischief)। (धारा 425)
- आपराधिक अतिचार (criminal trespasss) (धारा 441)
- मिथ्या साक्ष्य रचना (making false documents) (धारा 464)
- न्यायालय के अभिलेख (record) या लोक रजिस्टर आदि की कूट रचना। (धारा 466)
- मूल्यवान प्रतिभुमि, बिल आदि की कूटरचना। (धारा 467)
- छल के प्रयोजन से कुटरचना (forgery for cheating) (धारा 568)

सूचना औद्योगिकी अधिनियम, 2000 की निर्मित राष्ट्र संघ द्वारा सन् 1996 में पारित प्रास्ताव तथा उसके अधिनियम 'डॉ. मॉडल लॉ' के आधार पर की गई थी। जिसमे सदस्य देशों से अनुरोध किया गया था कि वे अपने देश में भी उक्त कानून पारित करें ताकि अन्तर्राष्ट्रीय स्तर पर होने वाले ई–वाणिज्य को विनियमित किया जा सके तथा सभी जगह एक समान साइबर कानून लागु हो। इस अधिनियम का मुल उदेश्य इलेक्ट्रानिक डाटा के विनिमय (exchange) तथा इलेक्ट्रानिक माध्यम से संचारित अन्य संव्यवहारों को विधिक मान्यता प्राप्त हो तथा कागजी पत्र–व्यवहार तथा दस्तावेजो के स्थान पर इलेक्ट्रानिक डाटा फाइलिंग से दस्तावेजों को संरक्षित किया जा सके।

सूचना प्रौद्योगिकी अधिनियम की परिधि में आने वाले अपराध (Offences covered under the Act)

सूचना प्रौद्योगिकी अधिनियम, 2000 के अन्तर्गत निम्नलिखित अपराधों के लिए दांडिक प्रावधान हैं–

- **अनधिकृत अधिनियम (Unauthorised access)–** अधिनियम की धारा 43 के अनुसार कोई व्यक्ति जो कम्प्यूटर, कम्प्यूटर सिस्टम या कम्प्यूटर नेटवर्क के स्वामी या प्रभारी (incharge) की अनुमति के बिना कम्प्यूटर, कम्प्यूटर सिस्टम या कम्प्यूटर नेटवर्क में अनधिकृत अभिगमन (unauthorised access) करता

है या अभिगमन को अभिप्राय करता (secures access) है तो वह इससे प्रभावित व्यक्ति (पीड़ित व्यक्ति) को प्रतिकर देगा जो एक करोड़ रूपये से अधिकराशि हो सकेगी।

धारा 43 के प्रयोजनों के लिए निम्नलिखित का कम्प्यूटर, कम्प्यूटर सिस्टम या कम्प्यूटर नेटवर्क में अनधिकृत पहूँच (अभिगमन) माना गया है–

- किसी कम्प्यूटर को अवैध रूप से स्विच–ऑन करनाः
- किसी कम्प्यूटर में संस्थापित साफ्टवेयर प्रोग्राम का अनिधकृत उपयोग करना
- फ्लॉपी–डिस्क (Floppy Disk) की अन्तर्वस्तु (contents) को अवैध रूप से देखना
- इन्टरनेट को अवैध तरीके से लॉग–ऑन करना

अनधिकृत अभिगत या पहूँच का अपराध उसी समय कारित हो जाता हैं जब डाटा, डाटा बेस या समाचार/सन्देश को डाउनलोड किया जाता है या अन्य कम्प्यूटर से उसकी प्रतिलिपि ली जाती है या अनधिकृत रूप से निकाली जाती है।

- **रिटर्न या जानकारी प्रस्तुत करने में विफल रहने का अपराध**–धारा 44 के अनुसार यदि कोई व्यक्ति इस अधिनियम या इसके अधीन निर्मित नियमों के अधीन कोई दस्तावेज, रिटर्न या रिपोर्ट कंट्रोलर या प्रमाणिकी–प्रधिकारी (Certifying Authority) को प्रेषित करने के लिए आबद्ध है, परन्तु वह इसमें व्यक्तिक्रम (कमनिसज) करता है या विफल रहता है तो उसे प्रत्येक विफलता के लिए जुर्माना जो डेढ़ लाख रूपये तक हो सकेगा, देना होगा तथा व्यक्तिक्रम की दशा में प्रत्येक दिन के लिए 5000/– का अर्थदण्ड देना होगा, जब तक कि व्यतिक्रम जारी रहता है।
- **अधिनियम के अन्तर्गत बनाए गए नियमों का उल्लंघन –** सूचना प्रौद्योगिकी अधिनियम की धारा 45 के अधीन अधिनियम के अन्तर्गत बनाए गए नियमों के उल्लंघन को अपराध माना गया है।
- **हेकिंग (Hacking) –** धारा 66 कम्प्यूटर सिस्टम को सदोष के साथ हेकिंग (छेडछाड़) को साइबर अपराध मानती है। जो भी किसी व्यक्ति या जन साधारण को सदोष हानि या क्षति कारित करने के आशय से किसी कम्प्यूटर में संग्रहीत की गई जानकारी/सुचना आदि को अविधिपूर्ण आशय से नष्ट करता है, मिटाता या बदलता है ताकि उसकी उपयोगिता कम हो जाए या समाप्त हो जाए, तो इसे 'हेकिंग' कहा जाएगा। जिसके लिए तीन वर्ष तक का कारावास या दो लाख रूपये तक अर्थदण्ड या दोनो से दण्डित किया जा सकेगा।

श्रेया सिंघल बनाम भारत संघ के वाद में उच्चतम न्यायालय ने सुचना प्रोद्योगिकी अधिनियम 2000 की धारा 66क को असांविधानिक घोषित कर दिया क्योंकि यह अभिव्यक्ति की स्वतन्त्रता को बाधित करती थी। तथपि उच्चतम न्यायालय ने अधिनियम की धारा 69क तथा वेबसाइट ब्लाकिंग नियमों (Website Blocking Rules) को वैध ठहराते हुए अभिकथन किया कि ये वेबसाइट मालिकों को उचित संरक्षण प्रदान करते है। न्यायालय ने कहा कि दुर्भाग्यवश वर्ष 2008 में संसद धारा 66क जल्दबाजी में बिना समुचित विचार–विमर्श के जोड़ी गई जिसके कारण अभिव्यक्ति की स्वतन्त्रता पर अनावश्यक रोक लगाई गई।

- **इलेक्ट्रानिक फार्म में अश्लील जानकारी का प्रकाशन – (Publishing Obesence Unformation in Electronic Form)–**इन्टरनेट पर अश्लीलता धारा 67 के अन्तर्गत दंडनीय अपराध है। इस धारा में प्रयुक्त शब्द 'प्रकाशन' से आशय जानकारी उपलब्ध करना या प्रख्यापित (Promulgate) करना या उसकी प्रतिलिपियॉ जनता में विक्रय हेतू उपलब्ध कराना है। वेबसाइट पर अश्लील सामग्री प्रदर्शित करना इस धारा के अधीन तीन वर्ष तक के कारावास या दो लाख रूपये अर्थदण्ड या दोनो से दण्डनीय है।

- **कपटपूर्ण उदेश्यो के लिए डिजीटल हस्ताक्षर प्रमाण पत्र प्रकाशित करना** (Publishing Digital Signature Certificate for Fraudulent Purposes) – अधिनियम की धारा 74 के अनुसार कोई भी व्यक्ति जो कपटपूर्ण आशय से जानबुझकर डिजीटल हस्ताक्षर प्रमाणपत्र तैयार करता है, प्रकाशित करता है या उपलब्ध कराता है इस धारा के अन्तर्गत दंडनीय होगा।

साइबर अपराधो की सांख्यिकी

अपराध सांख्यिकी के सन्दर्भ में वर्तमान में सुचना प्रौद्यागिकी तथा इन्टरनेट के बढ़ते प्रयोग के कारण तेजी से बढ़ रहे साइबर अपराधो के आंकड़ो का उल्लेख किया जाना आवश्यक प्रतीत होता है। विगत छ': वर्षो में सूचना प्रौद्योगिकी अधिनियम (Information Technology Avt, 2000) तथा भारतीय दण्ड संहिता के अन्तर्गत दर्ज किए गए विभिन्न साइबर अपराधों की स्थिति नीचे दी गई तालिका (ज्ंइसम) में दर्शाई गई है–

साइबर अपराधों की संख्या

वर्ष	सूचना प्रौद्योगिकी अधिनियम, 2000 के अन्तर्गत पंजीकृत हुए साइबर अपराधों की संख्या	भारतीय दण्ड संहिता, 1860 के अन्तर्गत पंजीकृत हुए साइबर अपराधों की संख्या	सइबर अपराधों का योग	गिरफ्तार किये गये व्यक्तियो की संख्या
2011	1791	422	2213	1630
2012	2876	601	3477	2071
2013	4356	1337	5693	3301
2014	7201	2421	9622	5752
2015	8045	3547	11592	8121
2016	9267	4653	13920	10435

साइबर अपराधों की स्थिति

सन् 2011 से 2016 के साइबर अपराधों सम्बन्धी आंकड़े यह दर्शाते है कि राज्यों एवं केन्द्र शासित प्रदेशों में इन अपराधों में सुचना प्रौद्योगिकी अधिनियम, 2000 के अधीन कारित अपराधों में औसतन परिवर्तनशीलता (Percentage variation) 60.1 प्रतिशत है जबकी भारतीय दण्ड संहिता, 1860 के अधीन कारित अपराधों में औसतन परिवर्तनशीलता 60.3 प्रतिशत है।

अन्य राज्यों की तुलना मे आन्ध प्रदेश, केरल, कर्नाटक, के दक्षिणी राज्यों तथा महाराष्ट्रो तथा गुजरात के पश्चिमी राज्यों में साइबर अपराध की घटनाएँ अधिक है। जहॉ तक केन्द्र शासित प्रदेशों का प्रश्न है, दिल्ली और चण्डीगढ़ में घटित साइबर अपराधों का प्रतिशत 90 है जबकि अन्य केन्द्र शासित प्रदेशों का प्रतिशत कुल मिलाकर 10 प्रतिशत मात्र है।

साइबर अपराधों के प्रति न्यायिक रूझान

राज्य बनाम मोहम्मद अफजल, (जो कि दिनांक 13 दिसम्बर 2001 को संसद में हुए आतंकवादी हमले का सरगना था) के वाद में दिल्ली उच्च न्यायालय ने स्वीकार किया है अभियोजन द्वारा साक्ष्य के रूप में प्रस्तुत किया गया डिजिटल सबूत अभियुक्त का साइबर अपराध सिद्ध करने में बहुत उपयोगी रहा है।

साइबर विधि – अन्तर्राष्ट्रीय परिप्रेक्ष्य (International Perspective of Cyber Law)

समस्त विश्वि के लिए साइबर अपराधियों ने कम्प्यूटर नेटवर्क के लिए एक गम्भीर खतरा उत्पन्न कर दिया है। अतः इस समस्या से विश्व–स्तर पर निपटने के लिए एक सर्वमान्य एण्टी–साइबर क्रिमिनल लॉ लागू किये जाने की आवश्यकता है। इस हेतु टोकियो (जापान) में सन् 1998 में सयुक्त राष्ट्र द्वारा विशेषज्ञों के एक कार्य–दल की बैठक आयोजित की गई थी ताकि साइबर आपराधिकता के निवारण एवं नियन्त्रण हेतू कारगर कदम उठाये जा सकें।

अन्तर्राष्ट्रीय स्तर पर यह अनुमान किया गया है कि यदि विश्व–देशों को सुचना प्रौद्योगिकी तथा कम्प्यूटर विज्ञान के विकास के फलस्वरूप होने वाले साइबर अपराधों में निरंतर हो रही वृद्धि को नियंत्रित रखना है तो इस हेतु संयुक्त प्रयास एवं सहयोग तथा एक–समान साइबर कानून पारित किये जाने की नितांत आवश्यकता है। यूरोपिय समुदाय (European Community) ने सन् 2002 में इलेक्ट्रानिक कामर्स सम्बन्धी निर्देश (Directives on e-commerece) लागू किये जिनमें इन्टरनेट मध्यस्थों (Internet Intermediaries) के लिए नियमों तथा उनके द्वारा किये जाने वाले अवैध कृत्यों एवं गतिविधियों को रोकने सम्बन्धी व्यवस्था दी गई है।

उपसंहार

ज्ञातव्य है कि विश्व में इन्टरनेट और कम्प्यूटर नेटवर्क के फैलाव के कारण नए प्रकार के अपराधों का जन्म हुआ है जिन्हें साइबर–अपराध कहा जाता है। इनका सर्वाधिक दुष्प्रभाव आर्थिक और सुरक्षा क्षेत्रो परपड़ा है जो साइबर–कपट (धोखा) तथा साइबर आतंकवाद के रूप में देश की आर्थिक दशा तथा सुरक्षा व्यवस्था को प्रभावित करते है।

केन्द्रीय सरकार ने दिसम्बर 2015 की एक जनहित याचिका के उत्तर में उच्चतम न्यायालय को सूचित किया था कि वह शीघ्र ही एक राष्ट्रीय साइबर क्राइम सहयोग केन्द्र (National Cyber Crime Coordination Centre) की स्थापना करने जा रही है जो केवल साइबर अपराध और राष्ट्रीय सुरक्षा से जुड़े मुदों पर विचार करेगा और अन्य दाण्डिक संस्थाओं से तालमेल रखते हुए इन अपराधों पर नियन्त्रण रखेगा परन्तु दिसम्बर 2016 तक इस केन्द्र की स्थापना नहीं हो सकी। जिसके लिए उच्चतम न्यायालय ने केन्द्र सरकार को आड़े हाथों लिया। केन्द्र सरकार राष्ट्रीय साइबर क्राइम सहयोग केन्द्र की स्थापना हेतु उच्चतम न्यायालय में शपथ पत्र प्रस्तुत कर चुकी है। केन्द्र सरकार ने दिनांक 30 अगस्त 2017 को उच्चतम न्यायालय को सुचित किया कि उसने राष्ट्रीय साइबर क्राइम को आपरेशन केन्द्र (NCCC) को प्रथम चरण पूरा कर लिया है और शीघ्र ही इसे पूरा कर लिया जाएगा।

सन्दर्भ ग्रन्थ सूची

- ✓ पार्थसारथी : साइबर क्राइम
- ✓ 'इन्फेक्टर्स' से आशय 'संक्रमणकारी' से है, अर्थात जो कम्प्यूटर प्रोग्राम का विनष्ट या अंवाछित रूप से परिवर्तित कर देते है।
- ✓ वियना वाइरस (Vienna Virus) डायरेक्ट एक्शन वाइरस का उदाहण है जबकि 'जेरूसलेम 185' रेसीडेंट–फाइल इन्फेक्टर वायरस का उदाहरण है।
- ✓ उदारणार्थ, स्पार्स इन्फेक्टर (Sparse Infactor) कम्पेनियन वायरस, आरमर्ड वायर (Armoured Virus) आदि।
- ✓ सिबर उल्रिच (Sieber Ulrich) The International Handbook of Computer Crime.
- ✓ राष्ट्रीय मानवाधिकार आयोग के महानिदेशक शंकर सेन द्वारा 'महिलाओं के विरूद्ध बढते अपराध' विषय पर दि. 11 मार्च 2014 को इन्जीनियरिंग तथा प्रबन्धन विश्वविद्यालय जयपुर में भाषण दिया गया। यही भाषण कलकत्ता इन्जीनियरिंग और प्रबन्ध विश्वविद्यालय में भी दिया गया था।
- ✓ Wilson Clay: Computer Attack & Cyber Terrorism (2003).
- ✓ शास्त्री पी. के. कम्प्यूटर साइंस एण्ड कम्प्यूटर फोरेन्सिक्स (2001)।
- ✓ अमरीकी कांग्रेस की वेबसाइट रिपोर्ट (2008) (विल्सन क्ले द्वारा प्रेषित)।
- ✓ Data diddling involves changing or erasing data in a subtle way, which makes it different to put the data back or be certain of its accurancy.

- ✓ कापीराइट अधिनियम 1957, को सन् 1994में संशोधित किया गया था जिसमें सन् 1999 में पुनः संशोधन किये गए जो 13 जनवरी 2000 से प्रभावी है।
- ✓ ए. आई. आर. 200 बम्बई 27.
- ✓ Satyam Infoway Ltd. Vs. M/s Sifynet Solution (p) Ltd. ए. आई. आर. 2004 सु. को. 3549
- ✓ 1990 पी. टी. सी. 19 दिल्ली 210.
- ✓ धारा 63–ए कापीराइट अधिनियम (संशोधित) 1999 दिनांक 13.01.2000 से प्रभावी ।
- ✓ इस अधिनियम की कमियों तथा दोषो को दूर करने के उदेश्य से सुचना प्रौद्योगिकी (संशोधन) अधिनियम 2008 (अधि. संख्या 10 सन् 2009)।
- ✓ अन्य प्रभावित कानून बैंकर्स बुक अधिनियम, 1891 तथा रिजर्व बैंक ऑफ इंडिया अधिनियम, 1934 में भी संशोधन किया गया। सूचना प्रौद्योगिकी अधिनियम, 2000 में चार अनूसुचियॉ है जिनमें क्रमशः दण्ड संहिता, साक्ष्य अधिनियम, बैकर्स बुक अधि. तथा रिजर्व बैंक ऑफ इंडिया अधि. में हुए संशोधनों का समावेश है।
- ✓ देखे, अनुसुची 1, सुचना प्रौद्योगिकी अधिनियम, 2000.
- ✓ डॉ. विश्वनाथ परांजपेः लीगल डाइमेन्शन्स ऑफ साइबर क्राइम्स एण्ड प्रोटेक्टिव लॉस इन इंडिया (2010)।
- ✓ सूचना प्रौद्योगिकी अधिनियम की सुसंगत धाराऍ 24, 25, 29, 30, 31, 32, 34 तथा 39 देखें।
- ✓ धारा 46 में एक नई उप धारा (1–ए) संशोधन अधिनियम 2008 द्वारा अन्तः स्थापित की गई है।
- ✓ उच्चतम न्यायालय द्वारा दि. 24 मार्च, 2015 को निर्णीत।
- ✓ धारा 69 (3)
- ✓ अधिनियम की धारा 2 (1) (म) में 'समुचित सरकार' की परिभाषा दी गई है जिसके अनुसार संविधान की अधिसुची, 7 की सुची 2 के वि ायों में राज्य सरकार तथा अन्य विषयों के लिए केन्द्र सरकार, 'समुचित सरकार' होगी।
- ✓ धारा 70–बी
- ✓ इस सम्बंध में देखे : सूचना प्रौद्योगिकी नियम 2000 का नियम 10 तथा 23.
- ✓ धारा 77(1) परन्तुक धारा 77 (1) Proviso.
- ✓ संशोधन अधिनियम, 2008 की धारा 39 द्वारा संशोधित तथा अक्टूबर 27, 2009 से प्रवृत।
- ✓ धारा 28 सुचना प्रौद्योगिकी अधिनियम, 2000।
- ✓ दण्ड प्रक्रिया संहिता 1973 की अनूसुची के अनुसार।
- ✓ धारा 46 (2) सूचना प्रौद्योगिकी अधिनियम, 2000.
- ✓ धारा 193 एवं 228 भारतीय दण्ड संहिता, 1860.
- ✓ धारा 195 तथा अध्ययन 26 दण्ड प्रक्रिया संहिता 1973 (1974 का अधिनियम 2).
- ✓ धारा 57 (6) सूचना प्रौद्योगिकी अधिनियम 2000.
- ✓ धारा 57 (5).
- ✓ धारा 58 (2).
- ✓ धारा 62.

- ✓ (1999) पी.टी. सी. (19) 2010 (दिल्ली) देखें टाटा एण्ड सन्स बनाम रामदास साफ्ट, 2004 (29) पी. टी. सी. 522 (दिल्ली)।
- ✓ ए. आई. आर. 2014 सु. को. 3540, देखे एक्वा मिनरल्स लि. बनाम प्रमोद बार्से ए. आई. आर. 2003 (दिल्ली) 463.
- ✓ (2003) बैंक केसेज (बी. सी.) 96 (इला.)।
- ✓ 2003 VII IN ADJ Delhi 1 (Cr. Apeal 80/2003).
- ✓ 2008 (3) एम. एल. जे. 406 (सु. को.)।
- ✓ मुख्य मेट्रोपोलिटन मजिस्ट्रेट इग्मोर द्वारा नवम्बर 5, 2004 को निर्णीत।
- ✓ पिटिशन संख्या 1276/2001 दिल्ली उच्च न्यायालय द्वारा मार्च 2003 में निर्णीत।
- ✓ ई–कामर्स पर यूरोपियन पार्लियामेंट एण्ड काउंसिल का निर्देश 2001/31/EC दिनांक जून 8, 2000.
- ✓ धारा 502 केलीफोर्निया दण्ड संहिता (संशोधित) 1997.
- ✓ अनुच्छेद 156–00–50 न्यूयार्क दण्ड संहिता, 1986.
- ✓ अनधिकृत अभिगमन तथा अनधिकृत उपांतरण दोनो के लिए ही दो वर्ष तक के कारावास की सजा दी जा सकती है।
- ✓ इस अपराध के लिए दस वर्ष तक के कारावास का दण्ड देय होगा।
- ✓ विनियम 369 मॉरीशन साइबर अधिनियम, 1998.
- ✓ Dr. Vishwanath Paranjape: Legal Dimensions of Crimes & Preventive Lawa (2010)p. 205.

♦❐♦