Shodh International: A Multidisciplinary International Journal (In Hindi)
https://www.eurekajournals.com/shodh.html
ISSN: 2581-3501

साइबर अपराध: सामाजिक सह वैधानिक सुरक्षा- एक समग्र अध्ययन

प्रवीण कुमार शुक्ला[1]

[1]सहायक आचार्य, विक्रमाजीत सिंह सनातन धर्म कालेज, नवाबगंज- कानपुर (उत्तर-प्रदेश) एवं एकेडमिक काउंसलर, इंदिरा गांधी नेशनल ओपन यूनिवर्सिटी, नई दिल्ली।

परिचय

वर्तमान समय में साइबर अपराध विश्व के लिए एक चुनौती बनकर उभरे हैं। वैश्वीकरण एवं सूचना प्रौद्योगिकी क्रांति के इस दौर में सामाजिक, सांस्कृतिक, आर्थिक, वैधानिक, प्रशासनिक, राजनैतिक एवं नैतिक मूल्यों का पतन देखने को मिल रहा है। कंप्यूटर का हेरफेर आमतौर पर कंप्यूटर नेटवर्क यानी इंटरनेट के माध्यम से होता है, 'साइबर अपराध' शब्द 'साइबरस्पेस' से विकसित हुआ है जो इंटरनेट को दर्शाता है। साइबर अपराध के पीड़ित को अपराधी द्वारा डिजिटल भेद्यता, निरक्षरता, आदि जैसे कुछ कारकों पर विचार करके चुना जा सकता है। 'साइबर अपराध' शब्द का प्रयोग पहली बार 1995 में सुस्मान और ह्यूस्टन[1] द्वारा किया गया था। साइबर अपराध शब्द को एक धारणा के बजाय आचरण और कार्यों के संग्रह के रूप में देखा गया था। पहला साइबर अपराध चार्ल्स बैबेज द्वारा 1820 में किया गया था। साइबर अपराध से सुरक्षा की अवधरणा हमें साइबर और कम्प्यूटर जनित अपराधों से सुरक्षा प्रदान करती है। अपने इन्टरनेट के डेटा को सुरक्षित बनाने के लिए एक सुरक्षा व्यवस्था का निर्माण किया गया है जिसे 'साइबर सुरक्षा'कहते है। 15 अगस्त 1995 में देश में पहली बार इंटरनेट का इस्तेमाल हुआ था। उस दौरान कुछ जगहों पर ही इंटरनेट की सुविधा देखने को मिल रही थी। लेकिन जैसे-जैसे इंटरनेट का विस्तार होता गया, साइबर अपराध की संख्या में सतत् बढ़ोत्तरी होने लगी। साइबर स्पेस सूचना परिवेश के भीतर एक वैश्विक डोमेन है, जिसमें परस्पर निर्भर सूचना प्रौद्योगिकी

[1]A brief study on Cyber Crime and Cyber Law's of India - International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 & p-ISSN: 2395-0072 Volume: 04 Issue: 06 June -2017(www.irjet.net)

अवसंरचना जैसे इंटरनेट, टेलीकॉम नेटवर्क, कंप्यूटर सिस्टम इत्यादि शामिल होते हैं। साइबर क्रान्ति के इस युग में कम्प्यूटर एवं इन्टरनेट के साथ ही रोबोट भी समाज में महत्वपूर्ण भूमिका निभाते हुए देखे जा रहे हैं। नूतन प्रौद्योगिकी के इस संजाल में अवसरों के साथसाथ अनेक नवीनतम चुनौतियाँ भी हैं। साइबर अपराध का क्षेत्र सोशल मीडिया (वाट्सएप, फेसबुक, ट्विटर) से लेकर ई-कॉमर्स एवं ई-बैंकिंग और राष्ट्रीय रक्षा-सुरक्षा तक बहुत व्यापक एवं महत्वपूर्ण है। वर्ष 2001 में ''साइबर-अपराध पर बुडापेस्ट अभिसमय'' में साइबर-अपराध[2],[3] को 21वीं सदी का सबसे बड़ा खतरा बताया गया था।

साइबर अपराध की परिभाषा

साइबर अपराध एक कंप्यूटर से संबंधित अपराध है। सूचना प्रौद्योगिकी अधिनियम, 2000[4] धारा 2(क) में 'अभिगम', धारा 2(ञ) में 'कंप्यूटर नेटवर्क', धारा 2(ट) में 'कंप्यूटर साधन', धारा 2(ण) में 'डाटा' और धारा 2(फ) में 'सूचना' को परिभाषित करता है। साइबर स्पेस शब्द का प्रयोग सबसे पहले विलियम गिब्सन ने वर्ष 1982 में अपनी पुस्तक 'न्यू रोमांसर' में किया था।[5] यह एक ऐसी आभासी दुनिया है, जहां बहुत सारी ऐसी गतिविधियां हैं जो आप देख नहीं सकते और यदि कुछ आप देख भी सकते हैं, तो उसे छू नहीं सकते। लेकिन इस आभासी दुनिया ने वास्तविक जगत् को जबर्दस्त ढंग से प्रभावित किया है। इसमें अनगिनत क्षमताएं हैं, अपार सम्भावनाएं हैं, ऐसा प्रतीत होता है कि आने वाला समय इंटरनेट और कम्प्यूटर के बिना सम्भव ही नहीं होगा। नब्बे के दशक के मध्य से हर क्षेत्र में इसका विस्तार बहुत तेजी से देखने को मिल रहा है। व्यापार, शासन-प्रणाली, शिक्षा, स्वास्थ्य, जैसी मूलभूत व्यवस्थायें भी साइबर स्पेस के दायरे से अछूता नहीं है। इलेक्ट्रॉनिक संचार और सॉफ्ट कॉपी जैसे माध्यमों का प्रयोग का प्रचलन बढ़ा है। इंटरनेट और कम्प्यूटर के माध्यम से विकास की गति तो तेज हुई है परन्तु पिछले दशकों से इस आभासी दुनिया में अपराध भी उससे ज्यादा तीव्र गति से बढ़े है, जो बहुत ही व्यापक और विध्वंसकारी सिद्ध हो रहे हैं, जिसे आमतौर पर साइबर क्राइम अथवा साइबर अपराध के नाम से भी जाना जाता है। कम्प्यूटर या इंटरनेट के माध्यम से घटित होने वाले अपराध साइबर-अपराध कहलाते हैं। साइबर अपराध श्वेतवासन अपराध का तेजी से उभरता एक

[2]01 जुलाई 2004 से प्रभावी है।

[3]European Treaty Series185-Cybercrime (Convention), 23.XI.2001

[4]Information technology law also called cyber law.

[5]https://www.britannica.com/topic/cyberspace The term "Cyberspace" was first used by the American-Canadian author William Gibson in 1982 in a story published in Omni magazine and then in his book Neuromancer.

नूतन प्रतिमान है। साइबर-क्राइम भौगोलिक एवं भौतिक सीमाओं से परे अन्तर्राष्ट्रीय, अन्तर्महाद्वीपीय अपराध है, जिसमें अनेक स्वरूप देखे जा सकते हैं, जैसे-साइबर-आतंकवाद, ई-मेल-स्पूफिंग, पोर्नोग्रापफी, डाटा डिडलिंग, मेल-हाईजेकिंग, वेब-हाईजेकिंग, वायरस-वार्म अटैक, क्रेडिट कार्ड फ्रॉड, मनी लाण्डरिंग, साइबर स्टाकिंग, ई-मेल बाम्बिंग, ट्रोजन हार्स इत्यादि।

यूरोपियन साइबर अपराध ट्रीटी काउंसिल के अनुसार[6] ''साइबर अपराध एक ऐसा अपराध है जो डेटा एवं कापीराइट के विरूद्ध की गयी आपराधिक गतिविधि है।

जेवियर गीज के अनुसार[7] ''साइबर अपराध कम्प्यूटर और इन्टरनेट के माध्यम से होने वाला अपराध है। जिसके अन्तर्गत जालसाजी, अनाधिकृत प्रवेश, चाइल्ड पोनोग्राफी और साइबर स्टाकिंग शामिल है।''

संयुक्त राष्ट्र के कम्प्यूटर अपराध कंट्रोल एण्ड प्रिवेंषन मेनुअल के अनुसार[8] ''जालसाजी, ठगी और अनाधिकृत प्रवेश को ही साइबर अपराध की परिभाषा में शामिल किया गया है। ''

साइबर अपराध के प्रकार

भारत इंटरनेट इस्तेमाल करने वाला चीन के बाद दुनिया का दूसरा[9] सबसे बड़ा देश बन गया है। एक अध्ययन के अनुसार वर्तमान में करीब 166 प्रकार के कम्प्यूटर जनित अपराध हैं, जिन्हें साइबर अपराध की श्रेणी में रखा जा सकता है। साइबर अपराध के कुछ प्रमुख प्रकार निम्नलिखित हैं:-

i. **हैकिंगः** इस प्रकार के साइबर अपराध में, एक व्यक्ति के कंप्यूटर के भीतर, उसकी व्यक्तिगत या संवेदनशील जानकारी को प्राप्त करने के उद्देश्य से पहुँच बनायी जाती है। इसमें अपराधी किसी व्यक्ति के कंप्यूटर में प्रवेश करने के लिए विभिन्न प्रकार के साफ्टवेयर का उपयोग करता है और पीड़ित व्यक्ति को यह पता नहीं चल सकता है कि उसका कंप्यूटर किसी दूरस्थ स्थान से एक्सेस किया जा रहा है। कई हैकर्स पासवर्ड क्रैक करने में सक्षम साफ्टवेर की मदद से संसाधनों तक पहुंच प्राप्त करने का प्रयास करते हैं। हैकर्स यह भी देख सकते हैं कि उपयोगकर्ता अपने कंप्यूटर पर क्या करते हैं। हैकर्स अपने

[6]https://www.scotbuzz.org/2020/09/cyber-crime.html
[7]https://www.scotbuzz.org/2020/09/cyber-crime.html
[8]https://www.scotbuzz.org/2020/09/cyber-crime.html
[9]https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/

कंप्यूटर पर उपयोगकर्ता की फाइलों को आयात या उसे एक्सेस भी कर सकते हैं। एक हैकर, उपयोगकर्ता की जानकारी के बिना उसके सिस्टम पर कई प्रोग्राम इंस्टाल कर सकता है। इस तरह के प्रोग्राम का उपयोग, पासवर्ड और क्रेडिट कार्ड जैसी व्यक्तिगत जानकारी को चोरी करने के लिए भी किया जा सकता है।

ii. **फिशि्गः** किसी को फर्जी ई-मेल भेजकर या प्रलोभन देकर ठगा जाता है। फर्जी मैसेज या फोन कॉल से एटीएम नम्बर या पासवर्ड की जानकारी प्राप्त करने का प्रयास किया जाता है।

iii. **साइबर बुलिंगः** फेसबुक,ट्विटर जैसे सोशल नेटवर्किंग साइट पर अशोभनीय टिप्पणी करना, धमकियां देना, मजाक उड़ाना या तंज कसना, शर्मिंदा करना आदि साइबर बुलिंग कहलाता है। यह साइबर उत्पीड़न भी कहलाता है।

iv. **स्पूफिंगः** इंटरनेट नेटवर्क पर कोई यूजर अपनी असली पहचान छुपाकर छद्म पहचान बनाकर अटैक या फ्रॉड करना, स्पूफिंग कहलाता है।

v. **स्पैमिंगः** अनावश्यक एवं बहु-संख्या में एक साथ मेल/ मैसेज भेजकर परेशान करनास्पैमिंग कहलाता है। ये सामान्यतया किसी अवैध वस्तुओं या सेवाओं को बेचने या ऑफर देने से संबधित होते हैं।

vi. **साइबर स्टाकिंगः** यह एक प्रकार का ऑनलाइन उत्पीड़न होता है, जिसमें पीड़ित को ऑनलाइन संदेशों और ई-मेल के जरिये परेशान किया जाता है। सामान्यतया ऑनलाइन उत्पीड़न करने वाले स्टाकर्स, पीड़ितों को जानते हैं और ऑफलाइन माध्यमों का सहारा लेने के बजाय, वे इलेक्ट्रानिक माध्यमों से उत्पीड़न करते हैं। यद्यपि वे देखते हैं कि साइबर स्टाकिंग का वांछित परिणाम नहीं निकल रहा है, तो वे साइबर स्टाकिंग के साथ-साथ ऑफलाइन स्टाकिंग का भी सहारा लेते हैं।

vii. **पहचान या पासवर्ड चोरीः** पहचान की चोरी को सामान्यतया दूसरे की व्यक्तिगत पहचान की जानकारी को उसके गैर-कानूनी उपयोग के रूप में परिभाषित किया जा सकता है। यह साइबर अपराध तब होता है जब कोई अपराधी, उपयोगकर्ता की व्यक्तिगत जानकारी तक पहुँच प्राप्त करते हुए धन की चोरी करने, गोपनीय जानकारी तक पहुंच बनाने आदि में धोखाधड़ी कारित करता है। ऐसे साइबर अपराधी पीड़ित के नाम पर फोन न. या आभासी खाता खोल कर पैसे की मॉग करते हैं। किसी आपराधिक गतिविधि की योजना बनाने के लिए पीड़ित के नाम का उपयोग करते हैं। हैकिंग के माध्यम से पीड़ित के पासवर्ड का पता लगाकर, सोशल मीडिया से व्यक्तिगत जानकारी प्राप्त कर सकते हैं, या आपको फिशिंग ई-मेल भी भेज सकते हैं।

viii. **डार्कनेट मार्केटः** इस प्रक्रिया से नशीले पदार्थ एवं ड्रग्स का अवैध आदान-प्रदान होता है। डार्क वेबसाइट 'सिल्करोड'[10] ने इस क्षेत्र में बहुत बड़ा बाजार विकसित कर लिया है।

ix. **बाल पोर्नोग्राफी और दुर्व्यवहारः** इसमें साइबर अपराधी, बाल पोर्नोग्राफी के उद्देश्य से चैट बाक्स के माध्यम से नाबालिगों को अपने साथ जोड़ते हैं। ऑनलाइन बाल पोर्नोग्राफी को भारत में साइबर अपराध के सबसे जघन्य रूप में देखा जाता है, जो भविष्य की पीढ़ी की सुरक्षा को खतरे में डाल रहा है। सिटी ऑफ यंगस्टाउन बनाम डे लॉरिटो (यूएसए, 1969)[11] के मामले में 'पोर्नोग्राफी' शब्द को परिभाषित किया गया है। परिभाषा निम्नवत् है-

'पोर्नोग्राफी' कामुक उत्तेजना पैदा करने के उद्देश्य से डिजाइन किए गए कामुक व्यवहार का चित्रण है। यह शब्द, कार्य या कृत्य हैं, जिसका उद्देश्य सेक्स भावनाओं को उत्तेजित करना होता है। यह कामुक प्रतिक्रिया को प्रोत्साहित करने के अपने एकमात्र उद्देश्य के साथ अक्सर वास्तविकता से भिन्न होता है। 'पोर्नोग्राफी' शब्द का अर्थ किसी काम या कला या रूप से है, जो सेक्स या यौन विषयों से संबंधित होता है। इसमें यौन गतिविधियों में शामिल पुरुष और महिला दोनों के चित्र/वीडियो शामिल होते हैं, और यह इंटरनेट की दुनिया में पहुँच के भीतर है।

आजकल पोर्नोग्राफी समाज के लिए एक तरह का व्यवसाय बन गया है क्योंकि लोग इसके जरिये आर्थिक लाभ प्राप्त करते हैं;उदाहरणार्थः बालीवुड अभिनेत्री शिल्पा शेट्टी के पति राज कुंद्रा। भारत में बाल पोर्नोग्राफी दण्डनीय है। सूचना प्रौद्योगिकी अधिनियम, 2000 और भारतीय दंड संहिता, 1860 बाल पोर्नोग्राफी के विरूद्ध सुरक्षा प्रदान करता है। इसके अंतर्गत पोषणीय मामलों में आईटी (संशोधन) अधिनयम, 2008 की धारा 67(क), एवं भारतीय दंड संहिता, 1860 की धारा 292, 293, 294, 500, 506और 509के अंतर्गत दण्ड का प्रावधान है।

X **साइबर आतंकवादः** यह साइबर अपराधों में सबसे गंभीर प्रकृति का साइबर अपराध माना जाता है। इसमें सरकार के विरूद्ध किये गए ऐसे साइबर अपराध, जिसमें सरकारी वेबसाइट या सैन्य वेबसाइट इत्यादि को हैक किया जाता है, शामिल हैं। जब सरकार के विरूद्ध साइबर अपराध किया जाता है, तो उसे उस राष्ट्र की संप्रभुता पर हमला और युद्ध की

[10]Silk Road was an online black market and the first modern darknet market. A darknet market is a commercial website on the dark web that operates via darknets such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the sale of legal products.

[11]"Decided September 10, 1969" City of Youngstown v. Deloreto, 19 Ohio App. 2d 267, (Ohio Ct. App. 1969)

कार्यवाही माना जाता है। ये अपराधी सामान्यतया आतंकवादी या अन्य देशों की दुश्मन सरकारें होती हैं।

भारत में साइबर अपराध की स्थिति

भारत में साइबर अपराध को रोकने हेतु सूचना प्रौद्योगिकी अधिनियम, 2000 पारित किया गया है। विश्व के 154 देशों में साइबर अपराध सम्बन्धी विधियॉ लागू है।[12] देश में साइबर अपराध और साइबर अपराधियों पर नियंत्रण रखने हेतु फली नरीमन[13] की अध्यक्षता में एक समिति गठित की गई थी, जो समय-समय पर साइबर अपराधों के सम्बन्ध में सरकार को प्रभावी सूचना उपलब्ध करातीथी। इस समिति द्वारा कम्यूनिकेशन कन्वर्जेन्स बिल, 2000 संसद में पेश किया था। यह बिल सूचना प्रौद्योगिकी, दूरसंचार एवंकेबल नेटवर्क को जोड़कर बनाया गया था। संयुक्त राष्ट्र संघ की महासभा द्वारा बताये गये मॉडल United Nations Commission on International Trade Law[14] (UNCITRAL)[15] के आधार पर भारत में साइबर-अपराधोंसे

[12]https://unctad.org/page/cybercrime-legislation-worldwide

[13]Fali Sam Nariman is the senior advocate to the Supreme Court of India. He has been awarded the Padma Bhushan (1991) and Padma Vibhushan (2007)

[14]The United Nations Commission on International Trade Law (UNCITRAL), established by the United Nations General Assembly by resolution 2205 (XXI) of 17 December 1966.

[15]According to the United Nations Commission on International Trade Law (UNCITRAL) 'electronic authentication' and 'signature' methods may be classified into the following categories;

1. Those based on the knowledge of the used or the recipient i.e passwords, personal identification numbers (PINs) etc.
2. Those bases on the physical features of the user i.e. biometrics.
3. Those based on the possession of an object by the user i.e. codes or other information stored on amagnetic card.
4. Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of ahand written signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, technologies currently in use include;

1. Digital Signature within a public key infrastructure
2. Biometric Device.
3. PINs
4. Passwords

निपटने के लिए सूचना प्रौद्योगिकी अध्निियम, 2000 लागू किया गया, जिसमें वर्ष 2008 में महत्वपूर्ण संशोधन किये गये। सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 में किये गये महत्वपूर्ण संशोधनों ने जहां इलेक्ट्रानिक दस्तावेज, इलेक्ट्रानिक हस्ताक्षर और कंप्यूटर तथा इंटरनेट के माध्यम से किए गए लेन-देन को विधिक पहचान दिलाई वहीं साइबर अपराधों को परिभाषित कर दोषियों के लिए पर्याप्त दण्ड के प्रावधान उपबंधित किए। संशोधित अधिनियम में महिलाओं की अमर्यादित दृश्य-प्रस्तुति ही नहीं बल्कि शाब्दिक अभद्रता के लिए भी दण्ड का प्रावधन किया गया। इस अधिनियम के अन्तर्गत कोई भी व्यक्ति यदि कम्प्यूटर या अन्य किसीइलेक्ट्रानिक संचार उपकरण के माध्यम से ऐसा संदेश भेजता है जो अश्लील हो, भ्रमाक हो तथा जिसका उद्देश्य किसी को असुविधा पहुंचाना, क्रोधित करना, अपमानित करना, इत्यादि हो, तो ऐसे संदेश के लिए दण्ड का प्रावधान किया हैं।

संयुक्त राष्ट्रसंघ द्वारा आयोजित अधिवेशन ''अपराध निवारण एवं आपराधिक न्याय'' विषय पर, ब्राजील के सल्वेडोर में 12-19 अप्रैल, 2010 के मध्य सम्पन्न हुआ। इस अधिवेशन में मुख्य चर्चा का विषय-क्षेत्र कम्प्यूटर-जनित अपराधों के कारण तथा निवारण पर ही केन्द्रित था तथा इस हेतु क्या उपाय किये जाएँ इस पर सदस्यों ने अपने विचार व्यक्त किये, लेकिन स्वदेशी हितों को ध्यान में रखते हुए हमारा देश एक 'मानक अन्तर्राष्ट्रीय विधि' पारित करने पर मतैक्य नहीं हो सका।[16]

भारत में गृह-मंत्रालय के अधीन कार्यरत संस्था'राष्ट्रीय अपराध रिकॉर्ड ब्यूरो'(एनसीआरबी) के अनुसार वर्ष 2020 में साइबर अपराध के 50,035 मामले दर्ज किए गए, जो वर्ष 2019में दर्ज मामलों की तुलना में 11.8 फीसदी अधिक है। एनसीआरबी के आंकड़ों के अनुसार, देश में साइबर अपराध की दर (प्रति एक लाख की आबादी पर घटनाएं) 2019 में 3.3 फीसदी से बढ़कर 2020 में 3.7फीसदी हो गईं। देश में 2019 में साइबर अपराध के मामलों की संख्या 44,735 थी, जबकि 2018 में यह संख्या 27,248 थी। वर्ष 2020 में ऑनलाइन बैंकिंग धोखाधड़ी के 4047 मामले, ओटीपी धोखाधड़ी के 1093 मामले, क्रेडिट-डेबिट कार्ड धोखाधड़ी के 1194 मामले, एटीएम से जुड़े 2160 मामले दर्ज किए गए। वर्ष 2020 में दर्ज साइबर अपराधों में से 60.2 फीसदी साइबर अपराध फर्जीवाड़ा (50,035 में से 30142 मामले) से जुड़े हुए थे। आंकड़ों के

5. Scanned handwritten signature
6. Signature by Digital Pen
7. Clickable "OK" or "I Accept" or "I Agree" click boxes

[16]https://www.struggleyourlife.com/2021/08/definition-of-cyber-crime-in-hindi.html

मुताबिक, यौन-उत्पीड़न के 6.6फीसदी (3293 मामले) और उद्दापन के 4.9 फीसदी (2440 मामले) दर्ज किए गए। साइबर अपराध के सर्वाधिक 11,097 मामले उत्तर प्रदेश में, 10741 कर्नाटक में, 5496 महाराष्ट्र में, 5027 तेलंगाना में और 3530 मामले असम में दर्ज किए गए। बहरहाल, अपराध की दर सबसे अधिक कर्नाटक में 16.2फीसदी थी, जिसके बाद तेलंगाना में 13.4 फीसदी, असम में 10.1फीसदी, उत्तर प्रदेश में 4.8फीसदी और महाराष्ट्र में यह दर 4.4फीसदी थी।[17]

सूचना प्रौद्योगिकी अधिनियम के अन्तर्गत साइबर अपराध से सम्बन्धित उपबन्ध

सूचना प्रौद्योगिकी अधिनियम में साइबर अपराधों से सम्बन्धित उपबन्ध निम्नवत् है-

धारा	अपराध का नाम	दण्ड
धारा 65	कंप्यूटर साधन दस्तावेजों से छेड़छाड़	कारावास 3 वर्ष तक या जुर्माने से, जो दो लाख तक का हो सकेगा या दोनों
धारा 66	कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश	कारावास 3 वर्ष तक या जुर्माने से, जो पांच लाख तक का हो सकेगा या दोनों
धारा 66 (क)	संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए	कारावास 3 वर्ष तक और जुर्माने से
धारा 66 (ख)	चुराये गये कंप्यूटर या अन्य किसी इलेक्ट्रानिक संचार युक्ति से सूचनाओं को बेईमानी से प्राप्त करना	कारावास 3 वर्ष तक या जुर्माने से, जो एक लाख तक का हो सकेगा या दोनों
धारा 66 (ग)	पहचान चोरी करने के लिए दण्ड	कारावास 3 वर्ष तक और जुर्माने से, जो एक लाख तक का हो सकेगा
धारा 66 (घ)	कंप्यूटर संसाधन का प्रयोग करके प्रतिरूपण द्वारा छल	कारावास 3 वर्ष तक और जुर्माने से, जो एक लाख तक का हो सकेगा
धारा 66 (ड़.)	निजता भंग करने के लिए दण्ड	कारावास 3 वर्ष तक या जुर्माने से, जो दो लाख तक का हो सकेगा या दोनों

[17]https://navbharattimes.indiatimes.com/india/cyber-crime-in-india-increased-by-118-in-2020-578-cases-of-fake-information-on-social-media/articleshow/86231616.cms

धारा 66(च)	साइबर आतंकवाद के लिए दण्ड	आजीवन कारावास तक
धारा 67	इलेक्ट्रानिक प्ररूप में आपत्तिजनक सूचनाओं काप्रकाशन	प्रथम दोषसिद्धि पर- कारावास तीन वर्ष तक और जुर्माने से, जो पांच लाख तक का हो सकेगा। द्वितीय या पश्चात्वर्ती दोषसिद्धि की दशा में- कारावास पांच वर्ष तक और जुर्माने से, जो दस लाख तक का हो सकेगा।
धारा 67 (क)	इलेक्ट्रानिक माध्यमों से लैंगिक प्रदर्शन या अश्लील सूचनाओं को प्रकाशित या प्रसारित करना	प्रथम दोषसिद्धि पर- कारावास पांच वर्ष तक और जुर्माने से, जो दस लाख तक का हो सकेगा। द्वितीय या पश्चात्वर्ती दोषसिद्धि की दशा में- कारावास सात वर्ष तक और जुर्माने से, जो दस लाख तक का हो सकेगा।
धारा 67 (ख)	इलेक्ट्रानिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या पारेषण, जिसमें बच्चों को कामवासना भड़काने वाली अवस्था में चित्रित्र किया गया हो	प्रथम दोषसिद्धि पर- कारावास पांच वर्ष तक और जुर्माने से, जो दस लाख तक का हो सकेगा। द्वितीय या पश्चात्वर्ती दोषसिद्धि की दशा में- कारावास सात वर्ष तक और जुर्माने से, जो दस लाख तक का हो सकेगा।
धारा 67 (ग)	मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दण्ड	कारावास तीन वर्ष तक और जुर्माने से
धारा 70	कंप्यूटर नेटवर्क संरक्षित प्रणाली तक अनाधिकृत रूप से पहुंच बनाने से संबंधित प्रावधान	कारावास दस वर्ष तक या जुर्माने से
धारा 71	डाटा या आंकड़ों का दुर्व्यपदेशन करना	कारावास दो वर्ष तक या जुर्माने से, जो एक लाख तक का हो सकेगा, अथवा दोनों।
धारा 72	गोपनीयता और निजता को भंग करने से संबंधित प्रावधान	कारावास दो वर्ष तक या जुर्माने से, जो एक लाख तक का हो सकेगा, अथवा दोनों।

धारा 72 (क)	संविदा की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान	कारावास तीन वर्ष तक या जुर्माने से, जो पांच लाख तक का हो सकेगा, अथवा दोनों।
धारा 73	अंकीय हस्ताक्षर का मिथ्या प्रकाशन	कारावास दो वर्ष तक या जुर्माने से, जो एक लाख तक का हो सकेगा, अथवा दोनों।

भारतीय दण्ड संहिता के अन्तर्गत साइबर अपराध से सम्बन्धित उपबन्ध-

धारा 292	इलेक्ट्रानिक रूप में अश्लील सामग्री का प्रकाशन, प्रसारण और विक्रय इत्यादि	प्रथम दोषसिद्धि पर- कारावास दो वर्ष तक और जुर्माने से, जो रू 2000/ तक द्वितीय या पश्चात्वर्ती दोषसिद्धि की दशा में- कारावास पॉच वर्ष तक और जुर्माने से, जो रू5000/तक
धारा 354ग	प्राइवेट कार्य में संलग्न किसी स्त्रियों को उन परिस्थितियों में देखना और चित्र खींचना	प्रथम दोषसिद्धि पर-कारावास न्यूनतम एक वर्ष तक जो अधिकतम तीन वर्ष तक हो सकेगी और जुर्माने से द्वितीय या पश्चात्वर्ती दोषसिद्धि की दशा में- कारावास न्यूनतम तीन वर्ष तक जो अधिकतम सात वर्ष तक हो सकेगी और जुर्माने से
धारा 354घ[18]	साइबर स्टाकिंग (पीछा करना)	प्रथम दोषसिद्धि पर- कारावास तीन वर्ष तक और जुर्माने से द्वितीय या पश्चात्वर्ती दोषसिद्धि की दशा में- कारावास पॉच वर्ष तक और जुर्माने से

[18]धारा 354(घ) भारतीय दंड संहिता, 1860 में किसी महिला को स्टाकिंग (पीछा करने) से सम्बंधित विधिक उपबन्ध उपबन्धित है।धारा354(घ) के अनुसार-

''ऐसा कोई पुरुष, जो

i. किसी स्त्री का उससे व्यक्तिगत अन्योन्यक्रिया को आगे बढ़ाने के लिए, उस स्त्री द्वारा स्पष्ट रूप से अनिच्छा उपदर्शित किये जाने के बावजूद, बारम्बार पीछा करता है और सम्पर्क करता है या संपर्क करने का प्रयत्न करता है; अथवा

ii. जो कोई किसी स्त्री द्वारा इन्टरनेट, ई-मेल या किसी अन्य प्रारूप की इलेक्ट्रानिक संसूचना का प्रयोग किये जाने को मानिटर करता है, पीछा करने (talking) का अपराध करता है।''

धारा 379	मोबाइल फोन से डेटा या कंप्यूटर हार्डवेयर इत्यादि चोरी करना[19]	तीन वर्ष तक का कारावास या जुर्माना; या दोनों
धारा 411	चुराई हुई संपत्ति का अभ्यासतः व्यापार करना	तीन वर्ष तक का कारावास या जुर्माना; या दोनों
धारा 419 और धारा 420	धोखाधड़ी के उद्देश्यों से पासवर्ड चोरी या फर्जी वेबसाइटों के निर्माण और साइबर धोखाधड़ी	साइबर अपराध की गंभीरता के आधार पर धारा 419 में तीन वर्ष साल तक का कारावास या जुर्माना और धारा 420 में सात वर्ष तक का कारावास या जुर्माना
धारा 465	साइबरस्पेस में, ई-मेल स्पूफिंग और कूटरचित दस्तावेज तैयार करना	दो वर्ष तक का कारावास या जुर्माना, या दोनों
धारा 468	छल के उद्देश्य से ई-मेल स्पूफिंग या ऑनलाइन जालसाजी के अपराध	सात वर्ष तक का कारावास या जुर्माना
धारा 469	इलेक्ट्रानिक रूपों के माध्यम से जालसाजी कर किसी व्यक्ति को बदनाम करने के उद्देश्य से व्यक्ति की प्रतिष्ठा या ख्याति को नुकसान पहुँचान	तीन वर्ष तक का कारावास या जुर्माना
धारा 500	इलेक्ट्रानिक माध्यमों जैसे ई-मेल इत्यादि के माध्यम से मानहानि कारित करना	दो वर्ष तक का कारावास या जुर्माना; या दोनों
धारा 504	ई-मेल या किसी अन्य इलेक्ट्रानिक माध्यमों से लोक-शांति भंग कराने के आशय से प्रकोपित करना	दो वर्ष तक का कारावास या जुर्माना; या दोनों
धारा 506	इलेक्ट्रानिक माध्यम से किसी व्यक्ति के शरीर, ख्याति या संपत्ति को अथवा उससे हितबद्ध किसी व्यक्ति की शरीर, ख्याति या संपत्ति को नुकसान पहुंचाना या नुकसान पहुंचाने की धमकी देना	दो वर्ष तक का कारावास या जुर्माना; या दोनों

[19]गगन हर्ष शर्मा बनाम स्टेट ऑफ महाराष्ट्र, 2018 इस मामले में, एक नियोक्ता ने पाया कि सॉफ्टवेयर और डेटा चोरी हो गए थे और कर्मचारियों को संवेदनशील जानकारी तक पहुंच प्रदान की गयी थी। नियोक्ता ने भारतीय दंड संहिताकी धारा 379, 408, और धारा 420 और आईटी एक्ट के प्रावधानों के अन्तर्गत मामला पंजीकृत कराया। न्यायालय के समक्ष प्रश्न यह था कि क्या पुलिस भारतीय दंड संहिताके अन्तर्गत मामला पंजीकृत कर सकती है या नही? उच्च न्यायालय ने निर्णीत किया कि भारतीय दंड संहिता के प्रावधानों के आधार पर मामला पंजीकृत नहीं किया जा सकता क्योंकि आईटी एक्ट का एक अधिभावी प्रभाव है।

धारा 509	इलेक्ट्रानिक माध्यम से किसी स्त्री की लज्जा का अनादर करना	तीन वर्ष तक का कारावास या जुर्माना
धारा 509ख[20]	इलेक्ट्रानिक साधनों द्वारा यौन उत्पीड़न	कारावास अवधि न्यूनतम छह माह, अधिकतम दो वर्ष तक एवं जुर्माना से

निष्कर्ष एवं सुझाव

यद्यपि यह सच है कि साइबर अपराध की गंभीरता दिन प्रति दिन बढती जा रही है, परन्तु हम सूझ-बूझ का पालन करके, फिशिंग हमलों, रैंसमवेयर, मैलवेयर, पहचान की चोरी और अन्य प्रकार के साइबर अपराध से स्वयं का बचाव कर सकते हैं। साइबर अपराध से बचाव हेतु सुझाव निम्नवत् है-

i. हमे अपरिचित लिंक या विज्ञापनों पर कभी भी क्लिक नहीं करना चाहिए।
ii. कंप्यूटर सिस्टम में एंटी-वायरस को अपडेटेड रखना चाहिए।
iii. सोशल नेटवर्किंग बेबसाइट एवं ई-मेल के पासवर्ड मजबूत रखना चाहिए। सुरक्षा की दृष्टि से पासवर्ड कम से कम आठ कैरेक्टर का, जिसमें लोअर केस लेटर्स, अपर केस लेटर्स, नंबर्स और स्पेशल कैरेक्टर्स का मिश्रण हो। अगर आप एक से अधिक अकाउंट्स का प्रयोग करते हैं, तो सभी के लिए अलग-अलग पासवर्ड का प्रयोग करें।
iv. इंटरनेट बैंकिंग और बैंकिग से जुड़े ट्रांजिक्शन आदि करने के लिए, जहॉ तक सम्भव हो अपने पर्सनल कम्प्यूटर, लैपटॉप या मोबाइल का ही इस्तेमाल करें। काम खत्म होते ही अकाउंट तुरन्त लॉग-आउट करना न भूलें और लॉगिन के दौरानकम्प्यूटर द्वारा यह पूछे जानेपर रिमेम्बर पासवर्ड या कीप लॉगिन में क्लिक कदापिन करें।
v. बैंकिंग यूजर नेम, लॉगिन पासवर्ड, ट्रांजिक्शन पासवर्ड, ओ.टी.पी, गोपनीय प्रश्नों या गोपनीय उत्तर को अपने मोबाइल, नोटबुक, डायरी, लैपटॉप या किसी कागज परन लिखें।
vi. सोशल साइट्स के अकाउंट को डिलीट करते समय सर्वप्रथम समस्त व्यक्तिगत जानकारी को डिलीट करें, तत्पश्चात् अकाउंट डी-एक्टिवेटया डिलीट करें।
vii. स्पैम या अनजान ई-मेल का उत्तर न दे, उसमें लगे संलग्नक को कभी खोल कर न देखें। उसमेंउपलब्ध कराये गये लिंक पर क्लिक न करें। इसमें वायरस या ऐसा प्रोग्राम हो सकता है, जिसको क्लिक करते ही कम्प्यूटर में वायरस आ सकता है,कम्प्यूटर में संरक्षित कोई फाइल/ डेटा डिलीट या करप्टकर सकता है।

[20]दण्ड विधि (छत्तीसगढ़ संशोधन) अधिनियम, 2013 प्रभावी तिथि- दिनांक 21 जुलाई 2015

viii. डिजिटल हस्ताक्षर का उपयोग सुरक्षित रूप से करने के लिए डोंगल को सदैव अपने पास सुरक्षित रखना चाहिए, पासवर्ड के साथही यूएसबी डिवाइस को भी सुरक्षित रखना चाहिए। यूएसबी में डेटा एक्सेस करने या कापी करने के दौरान यूएसबी सुरक्षा उत्पादोंमानकों का उपयोग करना चाहिए।

ix. ब्राडबैंड इंटरनेट एक्सेस के लिये निर्माता द्वारा अनुशंसित वैध वेबसाइटों से ही ड्राइवर डालनलोड करना चाहिए। मोडेम के साथ निर्माता द्वारा आपूर्ति की गई एडाप्टर डिवाइस का ही उपयोग करना चाहिए । सुरक्षित ब्राडबैंड इंटरनेट कनेक्शन का उपयोग करना चाहिए।

x. वाई-फाई के मामले में अज्ञात या अविश्वसनीय नेटवर्क से कनेक्ट नही करना चाहिए। वाई-फाई एक्सेस में पासवर्ड तकनीक का प्रयोग करना चाहिये। यदि किसी वेबसाइट पर कोई पॉपअप खुले और उसमे कुछ आकर्षक गिफ्ट या इनाम ऑफर करे, तो आपको अपनी व्यक्तिगत कोई भी जानकारी शेयर नही करना चाहिए जब तक स्वयं को सुरक्षात्मक दृष्टि सेआश्वस्त न कर लें।

xi. अपना पासवर्ड कभी भी अपने नाम, पता, गली नंबर, जन्म-तिथि, परिवार के सदस्यों के नाम, विद्यालय के नाम या अपने वाहनो के नंबर पर न बनाएं, जिसका दूसरों के द्वारा आसानी से अनुमान न लगाया जा सके।

अन्त में, साइबर अपराध से सिर्फ सूझ-बूझ का पालन करके ही बचाव कर सकते हैं।