खण्ड-7, अंक-1, वर्ष-2019, मु0प्र0 82-86
D.O.I.: 10.22445/avsp.v7i1.15

सूचना प्रौद्योगिकी अधिनियम 2000: एक वैज्ञानिक समीक्षा

राकेश कुमार सिंह
वैज्ञानिक–ई, गोविंद बल्लभ पंत राष्ट्रीय हिमालयी पर्यावरण एवं सतत् विकास संस्थान
हिमाचल क्षेत्रीय केंद्र, मौहल, कुल्लू–175126, हिमाचल प्रदेश, भारत
rksingh@gbpihed.nic.in

प्राप्त तिथि–27.08.2019, स्वीकृत तिथि–07.09.2019

सार– सूचना प्रौद्योगिकी अधिनियम–2000(इनफॉर्मेशन टेक्नोलॉजी एक्ट 2000), भारतीय संसद द्वारा मई, 2000 में पारित एक अधिनियम है जिसे सम्पूर्ण भारत में भारत के राजपत्र द्वारा 9 जून, 2000 को लागू कर दिया गया। सूचना प्रौद्योगिकी अधिनियम 2000 में 13 अध्यायों में विभक्त कुल 94 धाराएं हैं। भारत ने सूचना प्रौद्योगिकी अधिनियम–2000 को सूचना प्रौद्योगिकी(संशोधन) अधिनियम–2008 के माध्यम से काफी संशोधित किया तथा इस संशोधित अधिनियम को भारत के राजपत्र द्वारा 5 फरवरी, 2009 को भारत में लागू कर दिया गया। सूचना प्रौद्योगिकी(संशोधन) अधिनियम–2008 के तहत अध्याय–2 की धारा–3 में इलेक्ट्रॉनिक हस्ताक्षर की जगह डिजिटल हस्ताक्षर को जगह दी गई। इसके लिए धारा–2 में उपखंड(एच) के साथ उपखंड(एचए) को जोड़ा गया, जो सूचना के माध्यम की व्याख्या करता है। इसके अनुसार, सूचना के माध्यम से तात्पर्य मोबाइल फोन, किसी भी तरह का व्यक्तिगत डिजिटल माध्यम या फिर दोनों हो सकते हैं, जिनके माध्यम से किसी भी तरह की लिखित सामग्री, वीडियो, ऑडियो या तस्वीरों को प्रचारित, प्रसारित या एक से दूसरे स्थान तक भेजा जा सकता है ।

बीज शब्द– सूचना प्रौद्योगिकी अधिनियम 2000, सूचना प्रौद्योगिकी (संशोधन) अधिनियम 2008, साइबर अपराध, हैकिंग, आइडेंटिटी थेफ्ट, साइबरस्पेस, डिजिटल हस्ताक्षर

The Information Technology Act 2000: A Scientific Review

Rakesh Kumar Singh
Scientist-E, G.B. Pant National Institute of Himalayan Environment & Sustainable Development, Regional Centre Mohal, Kullu–175126, Himachal Pradesh, India
rksingh@gbpihed.nic.in

Abstract- The Information Technology Act 2000 is an Act passed by the Indian Parliament in May 2000, which came into force all over India on 9 June 2000 by the Gazette of India. The Information Technology Act 2000 has a total of 94 sections divided into 13 chapters. India significantly revised the Information Technology Act 2000 through the Information Technology (Amendment) Act 2008 and this amended Act was implemented in India by the Gazette of India on 5 February 2009. Under the Information Technology (Amendment) Act 2008, Section 3 of Chapter 2 replaced the electronic signature with a digital signature. For this, subdivision (HA) was added in Section 2 with subdivision (H), which explains the medium of information. Accordingly, the medium of information can be mobile phone, any kind of personal digital medium or both, through which any kind of written material, video, audio or photographs are promoted, broadcasted or transmitted from one place to another.

Key words- IT Act 2000, IT (Amendment) Act 2008, cyber crime, hacking, identity theft, cyber space, digital signature

1. **परिचय–** संयुक्त राष्ट्र की जनरल एसेंबली ने 30 जनवरी, 1997 को प्रस्ताव संख्या ए/आरइएस/51/162 के तहत यूनाइटेड नेशंस कमीशन ऑन इंटरनेशनल ट्रेड लॉ द्वारा अनुमोदित मॉडल लॉ ऑन इलेक्ट्रॉनिक कॉमर्स (इलेक्ट्रॉनिक कॉमर्स से संबंधित आदर्श कानून) को अपनी मान्यता दे दी। संयुक्त राष्ट्र की इस नियमावली में संवाद के आदान–प्रदान के लिए सूचना प्रौद्योगिकी या काग़ज़ के इस्तेमाल को एक समान महत्व दिया गया है और सभी देशों से इसे मानने की अपील की गई है। सूचना प्रौद्योगिकी अधिनियम, संयुक्त राष्ट्र की जनरल एसेंबली में 9 जनवरी, 2000 को पेश किया गया। सूचना प्रौद्योगिकी अधिनियम 2000 की प्रस्तावना में ही हर ऐसे लेनदेन को क़ानूनी मान्यता देने की बात उल्लिखित है, जो इलेक्ट्रॉनिक कॉमर्स के दायरे में आता है और जिसमें सूचनाओं के आदान–प्रदान के लिए सूचना

प्रौद्योगिकी का प्रयोग हुआ हो । इस क़ानून में सभी देशों से यह अपेक्षा की जाती है कि सूचना के आदान–प्रदान और उसके संग्रहण के लिए काग़ज़ आधारित माध्यमों के विकल्प के रूप में प्रयोग की जा रही तकनीकों से संबंधित कोई भी क़ानून बनाने या उसे संशोधित करते समय वे इसके प्रावधानों का ध्यान रखेंगे, ताकि सभी देशों के क़ानूनों में एकरूपता बनी रहे।[1]

2. **उद्देश्य और संबंधित मुद्दे**– आज का युग कम्प्यूटर और इंटरनेट का युग है। कम्पयूटर की मदद के बिना किसी बड़े काम की कल्पना करना भी मुश्किल है। ऐसे में अपराधी भी तकनीक के सहारे हाईटेक हो रहे हैं। वे जुर्म करने के लिए कम्प्यूटर, इंटरनेट, डिजिटल डिवाइसेज और वर्ल्ड वाइड वेब आदि का प्रयोग कर रहे हैं। ऑनलाइन ठगी या चोरी भी इसी श्रेणी का अहम गुनाह होता है। किसी की वेबसाइट को हैक करना या सिस्टम डेटा को चुराना ये सभी तरीके साइबर क्राइम की श्रेणी में आते हैं। साइबर क्राइम दुनिया भर में सुरक्षा और जाँच एजेंसियों के लिए परेशानी का सबब बन गया है। भारत में भी साइबर क्राइम मामलों में तेजी से इजाफा हो रहा है। सरकार ऐसे मामलों को लेकर बहुत गंभीर है। भारत में साइबर क्राइम के मामलों में सूचना तकनीक कानून 2000 और सूचना तकनीक (संशोधन) कानून 2008 लागू होते हैं। मगर इसी श्रेणी के कई मामलों में भारतीय दंड संहिता (आईपीसी), कॉपीराइट कानून 1957, कंपनी कानून, सरकारी गोपनीयता कानून और यहां तक कि आतंकवाद निरोधक कानून के तहत भी कार्रवाई की जा सकती है। आधुनिक क़ानून की शब्दावली में साइबर क़ानून का संबंध कंप्यूटर और इंटरनेट से है। विस्तृत संदर्भ में कहा जाए तो यह कम्प्यूटर आधारित सभी तकनीकों से संबद्ध है। सूचना प्रौद्योगिकी अधिनियम 2000 निम्नलिखित मुद्दों को संबोधित करता है–[2]

- इलेक्ट्रॉनिक दस्तावेजों को कानूनी मान्यता।
- डिजिटल हस्ताक्षर को कानूनी मान्यता।
- अपराध और उल्लंघन।
- साइबर अपराधों के लिए न्याय व्यवस्था।

3. **साइबर अपराध एवं अधिनियम**– अक्सर कम्प्यूटर में आए वायरस और स्पाईवेयर को हटाने पर लोग ध्यान नहीं देते हैं। उनके सिस्टम से होते हुए ये वायरस दूसरों तक पहुँच जाते हैं। हैकिंग, डाउनलोड, कंपनियों के अंदरूनी नेटवर्क, वाई–फाई कनेक्शनों और असुरक्षित फ्लैश ड्राइव, सीडी के जरिए भी वायरस फैल जाते हैं। वायरस बनाने वाले अपराधियों की पूरी एक इंडस्ट्री है, जिनके खिलाफ समय–असमय कड़ी कार्रवाई होती रही है। लेकिन आम लोग भी कानून के दायरे में आ सकते हैं। अगर उनकी लापरवाही से किसी के सिस्टम में कोई खतरनाक वायरस पहुँच जाए और बड़ा नुकसान कर दे। इस तरह के केस में आईटी (संशोधन) एक्ट 2008 की धारा 43 (सी), धारा 66, आईपीसी की धारा 268 और देश की सुरक्षा को खतरा पहुंचाने के लिए फैलाए गए वायरस पर साइबर आतंकवाद से जुड़ी धारा 66 (एफ) भी लगाई जाती है।

- **हैकिंग**– किसी कम्प्यूटर, डिवाइस, इंफॉर्मेशन सिस्टम या नेटवर्क में अनधिकृत रूप से घुसपैठ करना और डेटा से छेड़छाड़ करना हैकिंग कहलाता है। यह हैकिंग उस सिस्टम की फिजिकल एक्सेस और रिमोट एक्सेस के जरिए भी हो सकती है। जरूरी नहीं कि ऐसी हैकिंग के दौरान उस सिस्टम को नुकसान पहुँचा ही हो। अगर कोई नुकसान नहीं भी हुआ है, तो भी घुसपैठ करना साइबर क्राइम के तहत आता है, जिसके लिए सजा का प्रावधान है। आईटी (संशोधन) एक्ट 2008 की धारा 43 (ए), धारा 66 – आईपीसी की धारा 379 और 406 के तहत अपराध साबित होने पर तीन साल तक की जेल या पाँच लाख रुपये तक जुर्माना हो सकता है। किसी व्यक्ति, संस्थान या संगठन आदि के किसी सिस्टम से निजी या गोपनीय डेटा या सूचनाओं की चोरी करना भी साइबर क्राइम है। अगर किसी संस्थान या संगठन के अंदरूनी डेटा तक आपकी पहुँच है, लेकिन आप अपनी उस जायज पहुँच का इस्तेमाल संगठन की इजाजत के बिना, उसके नाजायज दुरुपयोग की मंशा से करते हैं, तो वह भी इसी अपराध के दायरे में आएगा।

- **आइडेंटिटी थेफ्ट**: किसी दूसरे व्यक्ति की पहचान से जुड़े डाटा, गुप्त सूचनाओं वगैरह का इस्तेमाल करना भी साइबर अपराध है। यदि कोई इंसान दूसरों के क्रेडिट कार्ड नंबर, पासपोर्ट नंबर, आधार नंबर, डिजिटल आईडी कार्ड, ई–कॉमर्स ट्रांजैक्शन पासवर्ड, इलेक्ट्रॉनिक सिग्नेचर वगैरह का प्रयोग करके शॉपिंग या धन की निकासी करता है तो वह इस अपराध में शामिल हो जाता है। जब आप किसी दूसरे शख्स के नाम पर या उसकी पहचान का आभास देते हुए कोई जुर्म करते हैं या उसका नाजायज फायदा उठाते हैं, तो यह जुर्म आइडेंटिटी थेफ्ट के दायरे में आता है। ऐसा करने वाले पर आईटी (संशोधन) एक्ट 2008 की धारा 43, 66 (सी), आईपीसी की धारा 419 लगाए जाने का प्रावधान है। जिसमे दोष साबित होने पर तीन साल तक की जेल या एक लाख रुपये तक जुर्माना हो सकता है।

- **पोर्नोग्राफी**: इंटरनेट के माध्यम से अश्लीलता का व्यापार भी खूब फलफूल रहा है। ऐसे में पोर्नोग्राफी एक बड़ा कारोबार बन गई है। जिसके दायरे में ऐसे फोटो, विडियो, टेक्स्ट, ऑडियो और सामग्री आती है, जो यौन, यौन कृत्यों और नग्नता पर आधारित हो। ऐसी सामग्री को इलेक्ट्रॉनिक ढंग से प्रकाशित करने, किसी को भेजने या किसी और के जरिए प्रकाशित करवाने या

भिजवाने पर पोर्नोग्राफी निरोधक कानून लागू होता है। दूसरों के नग्न या अश्लील वीडियो तैयार करने वाले या ऐसा एमएमएस बनाने वाले या इलेक्ट्रॉनिक माध्यमों से इन्हे दूसरों तक पहुँचाने वाले और किसी को उसकी मर्जी के खिलाफ अश्लील संदेश भेजने वाले लोग इसी कानून के दायरे में आते हैं। पोर्नोग्राफी प्रकाशित करना और इलेक्ट्रॉनिक जरियों से दूसरों तक पहुँचाना अवैध है, लेकिन उसे देखना, पढ़ना या सुनना अवैध नहीं माना जाता। जबकि चाइल्ड पोर्नोग्राफी देखना भी अवैध माना जाता है। इसके तहत आने वाले मामलों में आईटी (संशोधन) कानून 2008 की धारा 67 (ए), आईपीसी की धारा 292, 293, 294, 500, 506 और 509 के तहत सजा का प्रावधान है। जुर्म की गंभीरता के लिहाज से पहली गलती पर पाँच साल तक की जेल या दस लाख रुपये तक जुर्माना हो सकता है लेकिन दूसरी बार गलती करने पर जेल की सजा सात साल तक बढ़ सकती है।[3–4]

- **अन्य साइबर अपराधः** अधिकतर आपके इनबॉक्स या स्पैम बॉक्स में कई तरह के ईनाम देने वाले या बिजनेस पार्टनर बनाने वाले या फिर लॉटरी निकलने वाले मेल आते हैं। ये सभी मेल किसी दूसरे शख्स के ई–मेल या फर्जी ई–मेल आईडी के जरिए किए जाते हैं। किसी दूसरे के ई–मेल पते का इस्तेमाल करते हुए गलत मकसद से दूसरों को ई–मेल भेजना इसी अपराध की श्रेणी में आता है। हैकिंग, फिशिंग, स्पैम और वायरस, स्पाईवेयर फैलाने के लिए इस तरह के फर्जी ईमेल का इस्तेमाल अधिक होता है। ऐसा काम करने वाले अपराधियों का उद्देश्य ई–मेल पाने वाले को धोखा देकर उसकी गोपनीय जानकारी हासिल करना होता है। ऐसी जानकारियों में बैंक खाता नंबर, क्रेडिट कार्ड नंबर, ई–कॉमर्स साइट का पासवर्ड वगैरह आ सकते हैं। इस तरह के मामलों में आईटी कानून 2000 की धारा 77 बी, आईटी (संशोधन) कानून 2008 की धारा 66 डी, आईपीसी की धारा 417, 419, 420 और 465 लगाए जाने का प्रावधान है। दोष साबित होने पर तीन साल तक की जेल या जुर्माना हो सकता है। आज के दौर में सोशल नेटवर्किंग साइट्स खूब चलन में हैं। ऐसे में सोशल नेटवर्किंग वेबसाइटों, ई–मेल, चैट वगैरह के जरिए बच्चों या महिलाओं को तंग करने के मामले अक्सर सामने आते हैं। इन आधुनिक तरीकों से किसी को अश्लील या धमकाने वाले संदेश भेजना या किसी भी रूप में परेशान करना साइबर अपराध के दायरे में ही आता है। किसी के खिलाफ दुर्भावना से अफवाहें फैलाना, नफरत फैलाना या बदनाम करना भी इसी श्रेणी का अपराध है। इस तरह के केस में आईटी (संशोधन) कानून 2009 की धारा 66 (ए) के तहत सजा का प्रावधान है। दोष साबित होने पर तीन साल तक की जेल या जुर्माना हो सकता है।[5]

4. **अधिनियम में समाहित महत्वपूर्ण शब्द–** 2005 में प्रकाशित एडवांस्ड लॉ लेक्सिकॉन के तीसरे संस्करण में साइबरस्पेस शब्द को परिभाषित किया गया है। इसमें इलेक्ट्रॉनिक माध्यमों में फ्लोटिंग शब्द पर खासा जोर दिया गया है, क्योंकि दुनिया के किसी भी हिस्से से इस तक पहुँच बनाई जा सकती है। इसमें साइबर थेफ्ट (साइबर चोरी) शब्द को ऑनलाइन कम्प्यूटर सेवाओं के इस्तेमाल के परिप्रेक्ष्य में परिभाषित किया है। इस शब्दकोष में साइबर क़ानून की इस तरह व्याख्या की है, क़ानून का वह क्षेत्र, जो कंप्यूटर और इंटरनेट से संबंधित है और उसके दायरे में इंटेलेक्चुअल प्रॉपर्टी राइट्स, अभिव्यक्ति की स्वतंत्रता और सूचनाओं तक निर्बाध पहुंच आदि आते हैं। सूचना प्रौद्योगिकी अधिनियम 2000 में कुछ और बातों को परिभाषित किया गया है, जो इस प्रकार हैं, कम्प्यूटर से तात्पर्य किसी भी ऐसे इलेक्ट्रॉनिक, मैग्नेटिक, ऑप्टिकल या तेज़ गति से डाटा का आदान–प्रदान करने वाले किसी भी ऐसे यंत्र से है, जो विभिन्न तकनीकों की मदद से गणितीय, तार्किक या संग्रहणीय कार्य करने में सक्षम है। इसमें किसी कम्प्यूटर तंत्र से जुड़ा या सम्बंधित हर प्रोग्राम और सॉफ्टवेयर शामिल है।[6]

5. **साइबर अपराध के लिए दंड का प्रावधान (धारा 66–एफ)–** साइबर अपराध के मामलों में दंड विधान के लिए सूचना प्रौद्योगिकी अधिनियम–2000 में धारा 66–एफ को जगह दी गई है जिसके अनुसार

1. यदि कोईः

(अ) भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को भंग करने या इसके निवासियों को आतंकित करने के लिए–

(क). किसी अधिकृत व्यक्ति को कम्प्यूटर के प्रयोग से रोकता है या रोकने का कारण बनता है ।
(ख). बिना अधिकार के या अपने अधिकार का अतिक्रमण कर जबरन किसी कम्प्यूटर के प्रयोग की कोशिश करता है ।
(ग). कम्प्यूटर में वायरस जैसी कोई ऐसी चीज डालता है या डालने की कोशिश करता है, जिससे लोगों की जान को खतरा पैदा होने की आशंका हो या संपत्ति के नुक़सान का ख़तरा हो या जीवन के लिए आवश्यक सेवाओं में जानबूझ कर खलल डालने की कोशिश करता हो या धारा 70 के तहत संवेदनशील जानकारियों पर बुरा असर पड़ने की आशंका हो।

(ब) अनाधिकार या अधिकारों का अतिक्रमण करते हुए जानबूझ कर किसी कम्प्यूटर से ऐसी सूचनाएं प्राप्त करने में कामयाब होता है, जो देश की सुरक्षा या अन्य देशों के साथ उसके संबंधों के नज़रिए से संवेदनशील हैं या कोई भी गोपनीय सूचना इस इरादे के साथ हासिल करता है, जिससे भारत की सुरक्षा, एकता, अखंडता एवं संप्रभुता, अन्य देशों के साथ इसके संबंध, सार्वजनिक जीवन या नैतिकता पर बुरा असर पड़ता हो या ऐसा होने की आशंका हो, देश की अदालतों की अवमानना अथवा मानहानि होती हो या ऐसा होने की आशंका हो, किसी अपराध को बढ़ावा मिलता हो या इसकी आशंका हो, किसी विदेशी राष्ट्र अथवा व्यक्तियों

के समूह अथवा किसी अन्य को ऐसी सूचना से फायदा पहुँचता हो, तो उसे साइबर आतंकवाद का आरोपी माना जा सकता है।
2. यदि कोई व्यक्ति साइबर आतंकवाद फैलाता है या ऐसा करने की किसी साजिश में शामिल होता है तो उसे आजीवन कारावास की सजा सुनाई जा सकती है।

6. **सूचना प्रौद्योगिकी अधिनियम 2000 के अंतर्गत उल्लिखित अपराध–** मानव समाज के विकास के नज़रिए से सूचना और संचार तकनीकों की खोज को बीसवीं शताब्दी का सबसे महत्वपूर्ण अविष्कार माना जा सकता है। सामाजिक विकास के विभिन्न क्षेत्रों, ख़ासकर न्यायिक प्रक्रिया में इसके प्रयोग की महत्ता को कम करके नहीं आंका जा सकता, क्योंकि इसकी तेज़ गति, मानवीय ग़लतियों की कमी, कम ख़र्चीला होना जैसे गुणों के चलते यह न्यायिक प्रक्रिया को विश्वसनीय बनाने में अहम भूमिका निभा सकती है। इतना ही नहीं, ऐसे मामलों के निष्पादन में, जहाँ सभी संबद्ध पक्षों की शारीरिक उपस्थिति अनिवार्य न हो, यह सर्वश्रेष्ठ विकल्प सिद्ध हो सकता है। सूचना प्रौद्योगिकी अधिनियम 2000 के अंतर्गत उल्लिखित आरोपों की सूची निम्नवत है–[7]

- कम्प्यूटर संसाधनों से छेड़छाड़ की कोशिश–धारा 65
- कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश–धारा 66
- संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान–धारा 66 ए
- कम्प्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को ग़लत तरीक़े से हासिल करने के लिए दंड का प्रावधान–धारा 66 बी
- किसी की पहचान चोरी करने के लिए दंड का प्रावधान–धारा 66 सी
- अपनी पहचान छुपाकर कम्प्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुँच बनाने के लिए दंड का प्रावधान– धारा 66 डी
- किसी की निजता भंग करने के लिए दंड का प्रावधान–धारा 66 ई
- साइबर आतंकवाद के लिए दंड का प्रावधान–धारा 66 एफ
- आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े प्रावधान–धारा 67
- इलेक्ट्रॉनिक माध्यमों से सेक्स या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दंड का प्रावधान–धारा 67 ए
- इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो–धारा 67 बी
- मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दंड का प्रावधान–धारा 67 सी
- सुरक्षित कम्प्यूटर तक अनाधिकार पहुँच बनाने से संबंधित प्रावधान–धारा 70
- डाटा या आंकड़ों को ग़लत तरीक़े से पेश करना–धारा 71
- आपसी विश्वास और निजता को भंग करने से संबंधित प्रावधान–धारा 72 ए
- कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान–धारा 72 ए
- फर्जी डिजिटल हस्ताक्षर का प्रकाशन–धारा 73
- सूचना तकनीक क़ानून की धारा 78 में इंस्पेक्टर स्तर के पुलिस अधिकारी को इन मामलों में जांच का अधिकार हासिल है।

7. **भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान**

- ईमेल के माध्यम से धमकी भरे संदेश भेजना–आईपीसी की धारा 503
- ईमेल के माध्यम से ऐसे संदेश भेजना, जिससे मानहानि होती हो–आईपीसी की धारा 499
- फर्ज़ी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल–आईपीसी की धारा 463
- फर्ज़ी वेबसाइट्स या साइबर फ्रॉड–आईपीसी की धारा 420
- चोरी–छुपे किसी के ईमेल पर नज़र रखना–आईपीसी की धारा 463
- वेब जैकिंग–आईपीसी की धारा 383
- ईमेल का ग़लत इस्तेमाल–आईपीसी की धारा 500
- दवाओं को ऑनलाइन बेचना–एनडीपीएस एक्ट
- हथियारों की ऑनलाइन ख़रीद–बिक्री–आर्म्स एक्ट

भारत में साइबर क्राइम के मामलों में सूचना प्रौद्योगिकी अधिनियम 2000 और सूचना प्रौद्योगिकी (संशोधन) अधिनियम 2008 लागू होते हैं। मगर इसी श्रेणी के कई मामलों में भारतीय दंड संहिता (आईपीसी), कॉपीराइट कानून 1957, कंपनी कानून, सरकारी गोपनीयता कानून और यहां तक कि आतंकवाद निरोधक कानून के तहत भी कार्रवाई की जा सकती है। साइबर अपराध से संबंधित मामलों के लिए देश में साइबर

रेगुलेटरी कोर्ट की स्थापना की गई है। देश के कई बड़े शहरों में साइबर थाने खोले गए हैं। जिलों में साइबर सेल का गठन किया है, जो इन मामलों को सुनते हैं।

8. सन्दर्भ

1. https://www.wikipedia.org
2. https://meity.gov.in/content/information-technology-act-2000
3. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
4. https://www.wipo.int/edocs/lexdocs/laws/en/in/in024en.pdf
5. https://computerhindinotes.com/what-is-information-technology-act-2000
6. https://ehindistudy.com/2017/05/26/itact-2000-hindi-cyber-crime-hindi
7. https://www.drishtiias.com/hindi/daily-updates/daily-news-analysis/information-technology-1
8. https://aajtak.intoday.in/story/what-does-section-66a-of-it-act-say-1-804822.html