सूचना तकनीक अधिनियम (भारत)

सूचना तकनीक अधिनियम (Information Technology Act 2000) भारतीय संसद द्वारा पारित एक अधिनियम है जो 17 अक्टूबर 2000 को पारित हुआ। 27 अक्टूबर 2009 को एक घोषणा द्वारा इसे संशोधित किया गया।

इतिहास

सूचना तकनीक क़ानून 9 जनवरी 2000 को पेश किया गया था। 30 जनवरी 1997 को संयुक्त राष्ट्र की जनरल एसेंबली में प्रस्ताव संख्या 51/162 द्वारा सूचना तकनीक की आदर्श नियमावली (जिसे यूनाइटेड नेशंस कमीशन ऑफ इंटरनेशनल ट्रेड लॉ के नाम से जाना जाता है) पेश किए जाने के बाद सूचना तकनीक क़ानून, 2000 को पेश करना अनिवार्य हो गया था। संयुक्त राष्ट्र की इस नियमावली में संवाद के आदान-प्रदान के लिए सूचना तकनीक या काग़ज़ के इस्तेमाल को एक समान महत्व दिया गया है और सभी देशों से इसे मानने की अपील की गई है। सूचना तकनीक क़ानून, 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 तकनीक का इस्तेमाल हुआ हो. इलेक्ट्रॉनिक कॉमर्स सूचना के आदान-प्रदान और उसके संग्रहण के लिए काग़ज़ आधारित माध्यमों के विकल्प के रूप में इलेक्ट्रॉनिक माध्यम का इस्तेमाल करता है। इससे सरकारी संस्थानों में भी इलेक्ट्रॉनिक माध्यम से दस्तावेज़ों का आदान-प्रदान संभव हो सकता है और इंडियन पेनल कोड, इंडियन एविडेंस एक्ट 1872, बैंकर्स बुक्स एविडेंस एक्ट 1891 और रिज़र्व बैंक ऑफ इंडिया एक्ट 1934 अथवा इससे प्रत्यक्ष या परोक्ष रूप से जुड़े किसी भी क़ानून में संशोधन में भी इन दस्तावेज़ों का उपयोग हो सकता है।

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. 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 इस्तेमाल की जा रहीं 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. सूचना तकनीक क़ानून 2000 17 अक्टूबर 2000 को अस्तित्व में आया। इसमें 13 अध्यायों में विभक्त कुल 94 धाराएं हैं। 27 अक्टूबर 2009 को इस क़ानून को एक घोषणा द्वारा संशोधित किया गया. इसे 5 फ़रवरी 2009 को फिर से संशोधित किया गया, जिसके 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।

परिचय

आधुनिक क़ानून की शब्दावली में साइबर क़ानून का संबंध कंप्यूटर और इंटरनेट से है। विस्तृत संदर्भ में कहा जाए तो यह कंप्यूटर आधारित सभी तकनीकों से संबद्ध है। साइबर आतंकवाद के मामलों में दंड विधान के लिए सूचना तकनीक क़ानून, 2000 में धारा 66-एफ को जगह दी गई है।

66-एफ : साइबर आतंकवाद के लिए दंड का प्रावधान

1. यदि कोई-

> **(ए)** भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को भंग करने या इसके निवासियों को आतंकित करने के लिए-
> **क**. किसी अधिकृत व्यक्ति को कंप्यूटर के इस्तेमाल से रोकता है या रोकने का कारण बनता है।

ख. बिना अधिकार के या अपने अधिकार का अतिक्रमण कर जबरन किसी कंप्यूटर के इस्तेमाल की कोशिश करता है।

ग. कंप्यूटर 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 या-

(बी) अनाधिकार या अधिकारों का अतिक्रमण करते हुए जानबूझ कर किसी कंप्यूटर से ऐसी सूचनाएं हासिल 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 पहुंचता 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।

2005 में प्रकाशित एडवांस्ड लॉ लेक्सिकॉन के तीसरे संस्करण में साइबरस्पेस शब्द को भी इसी तर्ज पर 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 पहुंच बनाई जा सकती है। लेखक ने आगे इसमें साइबर थेफ्ट (साइबर चोरी) शब्द को ऑनलाइन कंप्यूटर 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 तकनीक क़ानून में कुछ और चीज़ों को परिभाषित किया गया है, जो इस प्रकार हैं, कंप्यूटर 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 कंप्यूटर तंत्र से जुड़ा या संबंधित हर प्रोग्राम और सॉफ्टवेयर शामिल है।

सूचना तकनीक क़ानून, 2000 की धारा 1 (2) के अनुसार, उल्लिखित अपवादों को छोड़कर इस क़ानून के प्रावधान पूरे देश में प्रभावी हैं। साथ ही उपरोक्त उल्लिखित प्रावधानों के अंतर्गत देश की सीमा से बाहर किए गए किसी अपराध की हालत में भी उक्त प्रावधान प्रभावी होंगे.

सूचना तकनीक क़ानून, 2000 के अंतर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान

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 इस्तेमाल की महत्ता को कम करके नहीं आंका जा सकता, क्योंकि इसकी तेज़ गति, कई छोटी-मोटी दिक्क़तों से छुटकारा, 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, जहां सभी संबद्ध पक्षों की शारीरिक उपस्थिति अनिवार्य न हो, यह सर्वश्रेष्ठ विकल्प सिद्ध हो सकता है। सूचना तकनीक क़ानून के अंतर्गत उल्लिखित आरोपों की सूची निम्नवत हैः

1. कंप्यूटर संसाधनों से छेड़छाड़ की कोशिश-धारा 65

2. कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश-धारा 66

3. संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान-धारा 66 ए

4. कंप्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को ग़लत तरीक़े से हासिल करने के लिए दंड का प्रावधान-धारा 66 बी

5. किसी की पहचान चोरी करने के लिए दंड का प्रावधान-धारा 66 सी

6. अपनी पहचान छुपाकर कंप्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुंच बनाने के लिए दंड का प्रावधान- धारा 66 डी

7. किसी की निजता भंग करने के लिए दंड का प्रावधान-धारा 66 इ

8. साइबर आतंकवाद के लिए दंड का प्रावधान-धारा 66 एफ

9. आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े प्रावधान-धारा 67

10. इलेक्ट्रॉनिक माध्यमों से सेक्स या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दंड का प्रावधान-धारा 67 ए

11. इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो-धारा 67 बी

12. मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दंड का प्रावधान-धारा 67 सी

13. सुरक्षित कंप्यूटर तक अनाधिकार पहुंच बनाने से संबंधित प्रावधान-धारा 70

14. डाटा या आंकड़ों को ग़लत तरीक़े से पेश करना-धारा 71

15. आपसी विश्वास और निजता को भंग करने से संबंधित प्रावधान-धारा 72 ए

16. कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान-धारा 72 ए

17. फर्ज़ी 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।

Punishments under sections—

66A – upto three years and fine

66B -upto three years or one lakh or both

66C- upto three years or one lakh or both

66D- upto three years or one lakh

66E- upto three years or two lakh or both

66F- life imprisonment(उमर कैद)

67- upto five years or ten lakh or both

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

1. ईमेल के माध्यम से धमकी भरे संदेश भेजना-आईपीसी की धारा 503

2. ईमेल के माध्यम से ऐसे संदेश भेजना, जिससे मानहानि होती हो-आईपीसी की धारा 499

3. फर्ज़ी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल-आईपीसी की धारा 463

4. फर्ज़ी वेबसाइट्स या साइबर फ्रॉड-आईपीसी की धारा 420

5. चोरी-छुपे किसी के ईमेल पर नज़र रखना-आईपीसी की धारा 463

6. वेब जैकिंग-आईपीसी की धारा 383

7. ईमेल का ग़लत इस्तेमाल-आईपीसी की धारा 500

8. दवाओं को ऑनलाइन बेचना-एनडीपीएस एक्ट

9. हथियारों की ऑनलाइन ख़रीद-बिक्री-आर्म्स एक्ट