IMPACT FACTOR 5.473(SJIF)
UPA NATIONAL E-JOURNAL
Interdisciplinary Peer-Reviewed Journal
ISSN 2455-4375

भारतातील माहिती आणि तंत्रज्ञानाचे कायदे आणि गुन्हे

प्रा. राजेश गेडाम
ग्रंथपाल
जिजामाता आर्टस कॉलेज, दारव्हा
Email - rajgedam1@gmail.com

प्रस्तावना :

आजचे युग हे माहिती आणि तंत्रज्ञानाचे युग म्हणुन ओळखले जाते. पृथ्वीवर अस्तीत्वात असलेल्या सर्वच क्षेत्रात माहिती तंत्रज्ञानाचा वापर केला जात आहे. हा वापर चांगल्या सोबतच वाईट कामासाठी सुध्दा केला जातो. परंतु माहिती आणि तंत्रज्ञानाचा उपयोग केवळ समाजहीतासाठीच व्हावा, यासाठी माहिती आणि तंत्रज्ञानाच्या वापराबाबत कायदे असणे गरजेचे झाले आहे. भारताचा माहिती तंत्रज्ञान कायदा (IT Act 2000) हा १७ ऑक्टोबर २००० सालापासुन अमंलात आला. आंतरराष्ट्रीय व्यापार विषय कामात याची आवश्यकता भासु लागली. जागतिक व भारतातील व्यापार, माहितीची सुरक्षा, सॉफ्टवेअर, ई—कॉर्मसचे डिजीटल संचलन, बौध्दिक संपदा, डेटा संरक्षण याकरीता हा कायदा तयार करण्यात आला.बौध्दिक संपदा हा आयटी कायदयाचा प्रमुख घटक आहे.

भारत सरकारच्या ईलेक्ट्रॉनिक आणि माहिती तंत्रज्ञान मंत्रालयानुसार :

महिती तं्रज्ञान कायदे इलेक्टॉनिक दस्तऐवजांना कायदेशीर मान्यता देतात आणि ई—फायलिंग, ई—कॉमर्स व्यवहारांना समर्थन देणारी रचना आणी सायबर क्राईम कमी करण्यासाठी, तपासण्यासाठी कायदेशीर सरंचना देखील प्रदान करते.

माहिती तं्रज्ञान कायदयाचे महत्व :

आजकाल माहिती तं्रज्ञान या कायद्याचे महत्व दिवसेदिवस खुप वाढत आहे. विविध क्षेत्रात तंत्रज्ञानाचा वापर करून धोकाधडीचे व्यवहार, चोरी व इतर विविध अनैतिक बाबींना आळा बसण्यासाठी निर्बंध असणे गरजेचे झाले आहे.

- इंटरनेटद्वारे होत असलेल्या सर्व व्यवहारांचा समावेश यामध्ये होतो.
- इंटरनेटद्वारे होत असलेल्या सर्व क्रियाकलपावर सतत लक्ष ठेवले जाते.
- सायबर कायद्यामुळे ई—व्यवहारांना कायदेशीर स्वरूप प्राप्त झाले
- विविध विलंबाने होणारी कामे झटपट व्हायला लागली.
- कादपत्रे सांभाळणे, जागेची गरज भासत नाही.
- शासकीय व खाजगी संस्थामध्ये सुलभता प्राप्त झाली.
- माहिती जशी च्या तशी संगणकामध्ये साठवणे शक्य झाली.
- इलेक्टॉनिक पध्दतीने डेटा, आकडेवारी, फाईल साठवणे शक्य झाले.

सायबर कायदयाचे कार्यक्षेत्र :

सायबर कायदयाचे मध्ये विविध प्रकारचे उददेश समाविष्ठ असतात. व्यक्ती आणि कंपन्या संगणक आणि इंटरनेट कसे वापरू शकतात यासाठी काहि नियम तयार करतात. तसेच काही कायदे इंटरनेटवरील अनैतिक क्रियाकलापांद्वारे लोकांना गुन्हेगारी चे बळी होण्यापासुन सरंक्षण देतात.

१.फसवणुक :

विविध ऑनलाईन कामे करतांना फसवणुकीपासुन संरक्षण करण्यासाठी ग्राहक सायबर कायद्यावर अवलंबुन असतात. डेटा चोरी, क्रेडिट कार्ड, कोअरबॅकिंग, ओळखीची चोरी, ऑनलाईन

होणारे इतर होणारे गुन्हे रोखण्यासाठी कायदे केले जातात. ओळख चोरी करणाऱ्या व्यक्तीला संघटित किंवा राज्य गुन्हेगारी आरोपांचा सामना करावा लागु शकतो. डिजीटल सीगनेचर सर्टिकेटवर अधिकारी वर्ग कार्यवाही करू शकतो. पिडीत व्यक्तीने आणलेली नागरी कार्यवाही होवु शकते. सायबर वकील इंटरनेट वापरून फसवणुक केल्याच्या आरोपांविरूध्द बचाव आणि खटला चालवण्याचे काम करतात.

२.कॉपीराईट :

माहिती आणी तंत्रज्ञानाच्या युगात मोठया प्रमाणात बौध्दिक माहिती हि इंटरनेटच्या माध्यमातुन मोठया प्रमाणात माहिती ऑनलाईन उपलब्ध आहेत. इंटरनेटमुळे कॉपीराईचे उल्लंघन सोपे झाले आहे. ऑनलाईनच्या माध्यातुन सुरवातीच्या दिवसामध्ये कॉपीराईटचे उल्लंघन करणे खुप सोपे होते. कॉपीराईट संरक्षण लादण्यासाठी कारवाई करण्यासाठी दोन्ही कंपन्या आणि व्यक्तींना वकिलाची आवश्यकता असते. कॉपीराईटचे उल्लंघन हे सायबर कायद्याचे एक क्षेत्र आहे जे व्यक्ती कंपन्यांच्या त्यांच्या स्वत:च्या सर्जनशील कार्यातुन नफा मिळविण्याच्या अधिकाराचे संरक्षण करते.

३.बदनामी :

अनेक व्यक्ती त्यांचे मत मांडण्यासाठी इंटरनेटचा वापर मोठया प्रमाणात करतात. ते आपले मत मांडतांना सत्य नसलेल्या गोष्टी सांगण्यासाठी जेव्हा इंटनेटचा वापर करून बदनामीची सीमा ओंलांडु शकते. बदनामी कायदे हे नागरी कायदे आहेत जे एखादया व्यक्तीला बनावट सार्वजनिक विधानापासुन वाचवतात. ज्यामुळे व्यवसाय किंवा एखाद्याच्या वैयक्तिक प्रतिष्ठेला हानी पोहोचु शकते. नागरी कायद्यांचे उल्लंघन करणारी विधाने करण्यासाठी लोक इंटरनेट वापरतात तेव्हा त्याला मानहानी कायदा म्हणतात. खराब एसएमएस पाठवणे.

४. छळ आणि पाठलाग :

बऱ्याच वेळा ऑनलाईन स्टेटमेंटस गुन्हेगारी कायद्यांचे उल्लंघन केले जावु शकतात. जेव्हा एखादी व्यक्ती ऑनलाईन दुसऱ्या कोणाबददल वारंवार धमकी देणारी विधाने करते तेव्हा दिवाणी आणि फौजदारी दोन्ही कायद्यांचे उल्लंघन होते. तेव्हा इंटअरनेट आणि इलेक्टॉनिक संप्रेषणाचा व इतर प्रकारांचा उपयोग करून लोकांचा छळ किंवा पाठलाग होतो तेव्हा सासबर वकिल खटला दाखल करून त्यांचा बचाव करतात.

५. भाषण स्वातंत्र्य :

अभिव्यक्ती स्वातंत्र्य हे राज्यघटनेने दिलेले आहे त्यामुळे सायबर कायद्याचे सुध्दा महत्वाचे क्षेत्र आहे. जरी सायबर कायदे काही विशिष्ठ वर्तन ऑनलाईन प्रतिबंधित करत असले तरी, भाषण स्वांतत्र्य कायदयामुळे लोकांना त्यांचे विचार मांडण्याची परवानगी मिळते. सायबर वकिलांनी त्यांच्या क्लायंटला अश्लीलतेला प्रतिबंधित करणाऱ्या कायदयाच्या मुक्त भाषणाच्या मर्यादांबदल सल्लादिला पाहिजे. सायबर वकिल त्यांच्या क्लायंटचा बचाव देखील करू शकतात तेव्हा क्लायेंटच्या कृतीमध्ये परवानगी योग्य मुक्त भाषण आहे की नाही याबददल वादविवाद होतो.

६. व्यापार रहस्ये :

ऑनलाईन व्यवहार करणाऱ्या कंपन्या त्यांच्या व्यापार गुपितांचे रक्षण करण्यासाठी सायबर कायदयावर अवलंबुन असतात. उदा. विविध सर्च इंजिने शोध परिणाम तयार करणारे अल्गोरिदम विकसीत करण्यासाठी बराच वेळ घालवतात. विविध माहिती शोधतांना सायबर कायदे या सर्च इंजिनला गुपीतांचे संरक्षण करण्यासाठी आवश्यकतेनुसार कायदेशिर कार्यवाही करण्यास मदत करतात. व्यापार करणाऱ्या कंपन्या व इतर शासकीय माहिती गुपीत राहण्याकरीता याकायदयाचा खुप आधार यांना होत असतो.

७. करार आणि रोजगार कायदा :

आपण बऱ्याच वेळेस विविध माहिती व इतरबाबी इंटरनेटच्या माध्यमातुन शोधत असतो त्याकरीता विविध संकेतस्थाळाचा वापर करत असतो तेव्हा अटी व शर्ती नासहमती दर्शविणारे बटण क्लिक करावे लागते. तेव्हा सायबर कायदा वापरला आहे असे गृहित धरल्या जाते. प्रत्येक संकेतस्थांच्या अटी व शर्ती असतात ज्या आहेत त्या कोणत्यातरी गोपनियतेशी संबधित आहेत.

सायबर कायद्याचे फायदे :

१. कायद्याद्वारे प्रदान केलेल्या कायदेशीर पायाभुत सुविधांचा वापर करून संस्था आता ई—कॉमर्स करण्यास सक्षम आहेत.

२. याकायद्यात डिजीटल स्वाक्षरींना कायदेशीर वैधता आणि मंजुरी देण्यात आली आहे.

३. यामुळे प्रमाणित अधिकारी होण्याच्या व्यवसायात डिजीटल स्वाक्षरी प्रमाणपत्रे जारी करण्यासाठी कॉर्पोरेट कंपन्यांच्या प्रवेशाचे दरवाजे खुले झाले आहेत.

४. यामुळे सरकारला वेबवर अधिसुचना जारी करण्यास अनुमती देते ज्यामुळे ई—गव्हर्नन्सची घोषणा होते.

५. कंपन्यांना किंवा संस्थांना कोणतेही फॉर्म, अर्ज किंवा इतर कोणतेही दस्तऐवज कोणत्याही कार्यालय, प्राधिकरण, संस्था किंवा योग्य सरकारच्या मालकिच्या किंवा नियंत्रित एजन्सीकडे ई—फॉर्मद्वारे विहित केलेल्या ई—फॉर्मद्वारे दाखल करण्याचा अधिकार देते.

६. आयटी कायदा सुरक्षेच्या मुदयावर देखील लक्ष देतो, जे इलेक्ट्रानिक व्यवहारांच्या यशासाठी खुप महत्वाचे आहेत.

सायबर गुन्हेगारी

इतर गुन्हा प्रमाणे सायबर गुन्हे किंवा संगणक केंदित गुन्हाहा एक गुन्हा आहे समजला जाते ज्यामध्ये संगणक आणि इंटरनेटवर्क समाविष्ठ आहे. एखाद्या गुन्हांच्या अंमलबजावणीसाठी संगणकाचा वापर केला असावा किंवा ते लक्ष्य असु शकते. फसवणुक करणे, ओळख चोरी करणे किंवा गोपनियतेचा भंग करणे यासारखे गुन्हेकरण्यासाठी संगणकाचा शस्त्र म्हणुन वापर करणे म्हणजे सायबर गुन्हे, वाणिज्य, करमणुक आणि सरकारी अशा प्रत्येक क्षेत्रात संगणक केंद्रस्थानी बनल्याने सायबर गुन्हयांचे, विशेषत : इंटरनेटद्वारे महत्व वाढले आहे. सायबर गुन्हयामुळे एखाद्या व्यक्तीची किंवा देशाची सुरक्षा आणि आर्थिक आरोग्य धोक्यात येवु शकते. सायबर गुन्हयांमध्ये अनेक प्रकारच्या क्रियाकलापांचा समावेश आहे. परंतुते सामान्यत:दोन श्रेणींमध्ये विभागले जावु शकतात.

१. संगणक नेटवर्क किंवा उपकरणांना लक्ष्य करणारे गुन्हे. याप्रकारच्या गुन्हयांमध्ये विविध धोके (जसे व्हायरस,बग इ.) आणि Denial of Service Attack (DoS) हल्ले यांचा समावेश होतो.

२. इतर गुन्हेगारी क्रियाकलाप करण्यासाठी संगणक नेटवर्क वापरणारे गुन्हे. या प्रकारच्या गुन्हयांमध्ये सायबर स्टॉकिंग, आर्थिक फसवणुक किंवा ओळख चोरी यांचा समावेश होतो.

सायबर गुन्हयांचे वर्गीकरण :

१. सायबर दहशतवाद :

सायबर दहशदवाद म्हणजे कॉम्प्युटर आणि इंटरनेटचा वापर करून हिंसक कृत्य करणे, ज्यामुळे जीवितहानी होते. यामध्ये सॉफ्टवेअर किंवा हार्डवेअरद्वारे नागरिकांच्या जीवाला धोका निर्माण करणाऱ्या विविध प्रकारच्या क्रियाकलापांचा समावेश असु शकतो. सर्वसाधारणपणे, सायबर दहशतवादाची व्याख्या सायबरस्पेस किंवा संगणक संसाधनांच्या वापराद्वारे केलेली दहशतवादाची कृती म्हणुन केली जावु शकते.

२. सायबर खंडणी :

जेव्हा एखादी वेबसाईट, ई—मेल सर्वर किंवा संगणक प्रणालीला वारंवार सेवा ना कारण्याची किंवा दुर्भावनापुर्ण हॅकर्सद्वारे इतर हल्याची धमकी दिली जाते तेव्हा सायबर खंडणी होते. हे हॅकर्स हल्ले थांबवण्याचे आणि संरक्षंण देण्याच्या आश्वासनाच्या बदल्यात मोठया रकमेची मागणी करतात.

३. सायबर युध्द :

विविध देशात वेगवेगळी सायबर प्रणाली विकसीत होत आहे त्यातुन वेगवेगळे व्हायरस/सॉफ्टवेअर सारखे निर्माण करून अनैतिक, आर्थीक, गुप्त माहिती चोरणे, एखाद्या मोठया नेटवर्कवर हल्ला/सायबर युध्द करणे. सायबरवॉरफेअर म्हणजे संगणक, ऑनलाईन नियंत्रण प्रणाली आणि नेटवर्कचा युध्दाच्या संदर्भात वापर किंवा लक्ष्य बनवलेजाते. यात सायबरहल्ले, हेरगिरी आणि तोडफोडीच्या धोक्यासंबधी दोन्ही आक्षेपार्ह आणि बचावात्मक ऑपरेशन आणि बचावात्क ऑपरेशन समाविष्ठ आहेत.

४. इंटरनेटफसवणुक :

इंटरनेट फसवणुक हा फसवणुकीचा एक प्रकार आहे ज्यात इंटरनेचा वापर करून त्यात माहिती लपवणे किंवा पैसे, मालमत्तेसाठी पीडीतांना फसवण्याचा उददेशाने चुकीची माहिती प्रदान करणे. इंटरनेट फसवणुक हा एक विशिष्ठ गुन्हा मानला जात नाही परंतु सायबरस्पेस मध्ये केलेल्या बेकायदेशीर कृतींचा समावेश होतो.

५. सायबरस्टाकिंग :

हासुध्दा एक प्रकारचा ऑनलाईनच्या माध्यमातुन केलेला छळच आहे ज्यामध्ये पीडीताला ऑनलाईन मेसेजेस आणि ई—मेलल्सचा त्रास होतो. याप्रकारात हे स्टॉकर्स त्यांच्या पीडीतांना ओळखतात आणि ऑफलाईन स्टॅकिंग ऐवजी ते इंटरनेटचा वापर करतात. तथापी, सायब रस्टॉलिंगचा अपेक्षित परिणाम होत नसल्याचे त्याच्या लक्षात आल्यास ते पीडितांचे जीवन अधिक दयनिय करण्यासाठी सायबर स्टॅकिंगसह ऑफलाईन स्टॅकिंग सुरू करतात.

सायबर क्राईम प्रतिबंध :

खालील काही मुददे आहेत ज्याद्वारे आपण सायबर गुन्हे रोखु शकतो.

१. मजबुत पासवर्ड वापरावा :

प्रत्येक खात्यासाठी वेगवेगळे पासवर्ड आणि वापरकर्तानाव संजोजन ठेवा आणि ते लिहुन ठेवण्याचा मोह टाळा. ब्रुट फोर्स अटॅक, रेनबो टेबल अटॅक इत्यादी काही आक्रमण पध्दती वापरून कमकुवत पासवर्ड सहजपणे क्रॅक केले जावु शकतात म्हणुन जटिल बनवा. त्यामध्ये लहान मोठे अक्षरे, संख्या, विशेष वर्ण, चिन्हे यांचे वापर करावा.

२. विश्वसनीय अॅटीव्हायरस वापर करावा :

संगणकामध्ये नेहमी विश्वसनीय आणि उच्च प्रगत अॅटीव्हायरस सॉफ्टवेअरचा वापर करावा. यामुळे आपल्या संगणकाची हाणी होणार नाही, हल्यापासुन बचाव होइल.

३. सॉफ्टवेअर नेहमी अपडेट ठेवणे :

आपण जेव्हा कोणतेही प्रोग्राम्स / सॉफ्टवेअर चा वापर करतो त्याचे वेळोवेळी नविन काही अपडेट उपलब्ध होत असतात. मागील आवृत्तीवर जर हल्ला करू शकत असेल तर नविन अपडेट उपलब्ध झाल्यामुळे त्याला सहजपणे हल्ला करणे शक्य होत नाही.

४. सोशल मिडियाचा खाजगीत वापरावा :

प्रत्येकाची सोशल मिडीयावर अकाउंटल्स असतात याची माहिती फक्त मित्रां व जवळच्या व्यक्ती पर्यन्त सिमीत ठेवा. तसेच फक्त जवळच्या मित्रांची विनंती मान्य करून मित्र बनवावे.

IMPACT FACTOR
5.473(SJIF)

UPA NATIONAL E-JOURNAL
Interdisciplinary Peer-Reviewed Journal

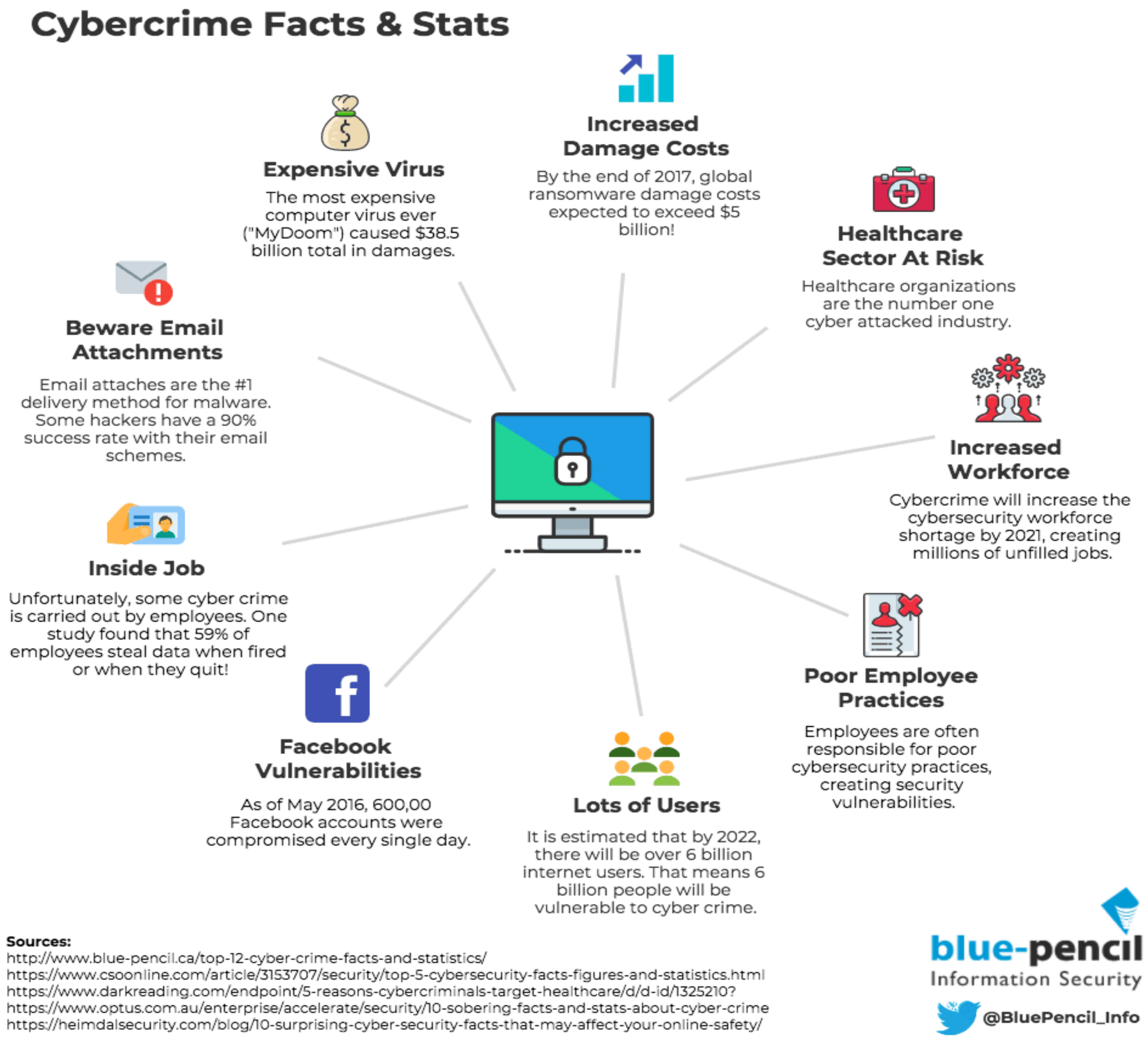
ISSN
2455-4375

५. सुरक्षित नेटवर्क वापरा :

सार्वजनिक वाय—फाय असुरक्षित आहेत. यानेटवर्कचा वापर करून आर्थिक किंवा कॉर्पोरेट व्यवहार करणे टाळावा.

६. स्पॅम ई—मेलमध्ये अटॅचमेंट कधिही उघडु नका :

विविध प्रकारच्या सायबर गुन्हयांमुळे संगणक संक्रमित होतो ते स्पॅम ई—मेलमधील अटॅचमेंटद्वारे होते. तुम्हाला माहित नसलेल्या प्रेषकाकडुन संलग्नित कधीही उघडु नका. वरील प्रकारची काळजी घेवुन प्रतिंबध लावला जावु शकतो.



समारोप :

पुथ्वीवर अस्तीत्वात असलेल्या सर्वच क्षेत्रात माहिती तंत्रज्ञानाचा वापर केला जात आहे. हा वापर चांगल्या सोबतच वाईट कामासाठी सुध्दा केला जातो. परंतु माहिती आणि तंत्रज्ञानाचा उपयोग केवळ समाजहीतासाठीच व्हावा, यासाठी माहिती आणि तंत्रज्ञानाच्या वापराबाबत भारतात माहिती तंत्रज्ञान कायदा (IT Act 2000) हा १७ ऑक्टोबर २००० सालापासुन अमंलात आला. देशाचे, जनतेचे, राष्ट्राचे कोणत्याही प्रकारचे नुकसान होवु नये याकरीता गैरमार्गाने वापर करणाऱ्यास आळा बसावा हा या कायदयाचा उद्देश होता. माहिती तंत्रज्ञान कायदयामुळे केवळ जनतेच्या हिताचे काम करण्यास शासनाला, कंपन्यांना, विविध एजन्सीजला याचेमुळे संरक्षण मिळाले आहे.

परंतु आजकाल माहीती तत्रज्ञांनाचा गैरवापर करून ऑनलाईन फ्रॉड, कोअर बॅंकिंग, बदनामी, सामाजिक कलह निर्माण केले जातात. अशा सामाजिक अहीतकारक घटकांना आळा बसावा, याकरीता अशा कायदयातील त्रुटी दूर करणे आवश्यक आहे. तसेच समाजातील सर्व घटकांना माहीती तंत्रज्ञानाच्या वापरासंदर्भात परिपूर्ण होणे काळाची गरज आहे. तेव्हाच असे कायदयाची यशस्वी अंमलबजावणी होते,असे आपण म्हणू शकतो

संदर्भ :

- Amita Varma., Cyber Crime in India,Central Law Publications.
- IGNOU MCS-215 - Security and Cyber Laws, Latest Help Book Edition
- Sameena Bazmoul., Cyber Law & Crime, Hyderabad: ASIA Law House
- https://mr.phondia.com/information-technology-act-2000-in-marathi/access on 20april2022
- Information Technology Act 2000 | Ministry of Electronics and Information Technology, Government of India (meity.gov.in) access on 18April2022