IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Privacy And Data Protection In Cyberspace – A Critical Analysis Of Data Protection Laws In India

ADITYA AGARWAL

LLM Student

Amrit Law College, Dhanauri, Roorkee

सार

यह पेपर साइबरस्पेस में हमारे डेटा की सुरक्षा से संबंधित कानूनों से संबंधित है। साइबरस्पेस एक ऐसा क्षेत्र है जो तुरंत विकसित हो रहा है और हमारी दिन-प्रतिदिन की गतिविधियों में प्रत्येक व्यक्ति की घरेलू आवश्यकता बन गया है। सभी प्रकार की व्यावसायिक और व्यक्तिगत गतिविधियाँ ऑनलाइन आयोजित की जाती हैं। साइबरस्पेस में हम सभी का समानांतर जीवन है। आजकल जब भी हमें आवश्यकता होती है, हमें किसी भी स्थान से किसी से संबंधित डेटा या जानकारी तक पहुंच प्राप्त होती है। प्रौद्योगिकी के इस उद्भव ने हमारी व्यक्तिगत और गोपनीय जानकारी के लिए ई-खतरे को भी जन्म दिया है।

वैश्वीकरण ने विभिन्न देशों की विकासशील पूर्व शर्त के अनुसार, पूरी दुनिया में नवाचार को स्वीकृति दी है। इंटरनेट के उपयोग और ऑनलाइन संग्रहीत और प्रसारित डेटा की मात्रा के आधार पर उचित कानून के साथ संरक्षित करने की आवश्यकता है। लेखक भारत में विशिष्ट डेटा संरक्षण कानूनों की आवश्यकता के साथ-साथ डेटा की सुरक्षा और डेटा संरक्षण से संबंधित मौजूदा प्रावधानों में इन दिनों सामने आने वाले विभिन्न मुद्दों और चुनौतियों पर प्रकाश डालेगा।

कीवर्ड: साइबर स्पेस, डेटा, सूचना, गोपनीयता, सुरक्षा, विधान।

परिचय

जैसा कि हम एक ऐसी दुनिया में रहते हैं जो निजी और सार्वजनिक गतिविधियों और आवश्यकताओं दोनों में विभिन्न रूपों में प्रौद्योगिकियों में उन्नत है। हमारे डेटा की सुरक्षा के लिए प्रासंगिक कानून और नियम प्रदान करना भी राज्य का कर्तव्य है। डेटा सुरक्षा को देश के नियमों, विनियमों और गोपनीयता नीतियों के सेट के रूप में पढ़ा जा सकता है जो किसी भी व्यक्ति की व्यक्तिगत जानकारी के उपयोग को कम करने का इरादा रखता है। अपने लोगों और आम जनता के काम को आसान बनाने वाली तकनीक का उपयोग अब निजी या सार्वजनिक संगठनों के कामकाज के लिए व्यक्तिगत जानकारी एकत्र करने के लिए किया जा रहा है। हालाँकि भारत का संविधान मौलिक अधिकार के रूप में गोपनीयता पर स्पष्ट रूप से स्पष्ट नहीं है, हालाँकि संविधान के अनुच्छेद 19 और 21 के तहत अदालतों ने निजता के अधिकार की गारंटी दी है। पुट्टास्वामी (सेवानिवृत्त) में माननीय सर्वोच्च न्यायालय &

Anr बनाम भारत संघ और Ors[1], ने माना कि निजता का अधिकार भारत के अनुच्छेद 14, 19 और 21 के तहत मौलिक अधिकार के रूप में संरक्षित है[2]।

डेटा गोपनीयता-आवश्यकता एवं महत्व

आवश्यकता और महत्व डेटा गोपनीयता या सूचना गोपनीयता को एक ऐसे क्षेत्र के रूप में समझा जा सकता है जिसका मुख्य फोकस उस डेटा को बनाए रखना और संरक्षित करना है जिसे प्रकृति में संवेदनशील माना जाता है। डेटा गोपनीयता केवल व्यक्तिगत डेटा की सुरक्षा और संरक्षण नहीं है बल्कि इससे कहीं अधिक है। व्यक्तिगत डेटा को वैध और नैतिक तरीके से प्रबंधित करना संगठनों का दायित्व है, इसका मतलब है कि मालिक की सहमति के बिना, उनका डेटा तीसरे पक्ष के साथ साझा नहीं किया जाना चाहिए। संबंधित संगठनों का यह कर्तव्य है कि वे एकत्र किए जा रहे डेटा और उन डेटा के उपयोग के उद्देश्य पर अपने ग्राहकों के साथ सावधान और स्पष्ट रहें। हालाँकि संगठन डेटा उल्लंघनों को पहचानते हैं और साइबर हमलों के बड़े खतरे से अच्छी तरह वाकिफ हैं, फिर भी वे सुरक्षा की आवश्यकता पर लापरवाही बरतते हैं, जिसे व्यक्तियों के "अधिकार और स्वतंत्रता के रूप में जाना जाता है। संगठन अपने ग्राहक के व्यक्तिगत डेटा को बनाए रख सकते हैं, इसे इस तरह से निजी बनाए रख सकते हैं कि यह ग्राहकों की पहचान का खुलासा नहीं करेगा, साथ ही साथ संगठन की प्रतिष्ठा भी सुरक्षित रहेगी एक सरकारी एजेंसी, निगम, स्कूल या अस्पताल में डेटा उल्लंघन गुप्त जानकारी डाल सकता है, मालिकाना डेटा, छात्रों या मरीज़ों की जानकारी उन आपराधिक हाथों में है जो पहचान की चोरी कर सकते हैं।

व्यक्तिगत और संवेदनशील व्यक्तिगत डेटा के बीच अंतर

व्यक्तिगत डेटा

व्यक्तिगत डेटा को उन सूचनाओं के रूप में पहचाना जा सकता है जो किसी व्यक्ति की पहचान प्रदान करने में मदद करती हैं। इसमें व्यक्ति का नाम, उसका खाता नंबर या अन्य डिजिटल तरीकों जैसे उसके सिस्टम का आईपी पता, उसका जीपीएस या उपयोगकर्ता नाम आदि शामिल हो सकते हैं।

संवेदनशील व्यक्तिगत डेटा

संवेदनशील व्यक्तिगत डेटा को उन सूचनाओं के रूप में समझा जा सकता है जो किसी व्यक्ति के प्रकट होने या गलत तरीके से संभाले जाने की स्थिति में उसे नुकसान पहुंचा सकती हैं। संवेदनशील व्यक्तिगत डेटा के कुछ उदाहरण निम्नलिखित हैं:

नस्लीय या जातीय मूल (रेसियल या एथनिक ओरिजिन)।राजनीतिक या धार्मिक विश्वास, ट्रेड यूनियन सदस्यता, शारीरिक या मानसिक स्वास्थ्य, यौन जीवन या यौन अभिविन्यास, आपराधिक अपराध और अदालती कार्यवाही, वॉयस रिकॉर्डिंग, स्वास्थ्य रिकॉर्ड, राजनीतिक संबद्धता, बायोमेट्रिक्स[3]।

व्यक्तिगत डेटा और संवेदनशील व्यक्तिगत डेटा के बीच अंतर को समझना आवश्यक है क्योंकि संवेदनशील व्यक्तिगत डेटा को संभालते समय अतिरिक्त देखभाल की आवश्यकता होती है।

प्रोसेसर बनाम नियंत्रक

नियंत्रक:

डेटा नियंत्रक उन उद्देश्यों को निर्धारित करता है जिनके लिए और वे साधन जिनके द्वारा व्यक्तिगत डेटा संसाधित किया जाता है। इसका मतलब यह है कि वे इस बारे में निर्णय लेते हैं कि कौन सी जानकारी ली गई है और क्यों[4]?

---

[1] (2017) 10 एससीसी 1

[2] भंडारी, वृंदा; काक, अंबा; परशीरा, स्मृति; रहमान, फैजा। "पुत्तास्वामी का विश्लेषण: सुप्रीम कोर्ट का गोपनीयता निर्णय।"। इंद्रस्त्र ग्लोबल। 003: 004. आईएसएसएन 2381-3652

[3] https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/data-privacy-egypt-what-you-need-know-en.pdf पर उपलब्ध है

[4] वही

प्रोसेसर:

डेटा प्रोसेसर केवल नियंत्रक की ओर से व्यक्तिगत डेटा को संसाधित करता है। डेटा प्रोसेसर आमतौर पर कंपनी के बाहर एक तीसरा पक्ष होता है। यदि कोई प्रोसेसर कुछ या सभी प्रोसेसिंग को किसी अन्य संगठन को उपठेके पर देता है, तो बाद वाले को सब-प्रोसेसर[5] कहा जाता है।

डेटा नियंत्रक

मैं अंततः अपने स्वयं के अनुपालन और अपने प्रोसेसर के अनुपालन के लिए जिम्मेदार हूं। मेरे कर्तव्यों में सूचना आश्वासन मानकों का अनुपालन, लोगों के विशेषाधिकारों पर प्रतिक्रिया करना, सुरक्षा प्रयासों को कायम रखना, सूचना प्रवेश की निगरानी करना और डेटा को पर्याप्त सुरक्षा देने वाले प्रोसेसर के साथ जुड़ना शामिल है।

प्रोसेसर

मैं जो जानकारी तैयार कर रहा हूं उस पर मेरा स्वशासन कम है, हालांकि किसी भी मामले में मेरी प्रत्यक्ष वैध प्रतिबद्धताएं हो सकती हैं। बंद मौके पर कि मैं एक उप-प्रोसेसर से जुड़ता हूं, मैं उप प्रोसेसर के अनुपालन के लिए नियंत्रक के लिए बाध्य हो सकता हूं। मेरे दायित्वों में बाहरी समझौतों में निर्धारित आपके नियंत्रक दिशानिर्देशों के साथ निरंतरता, सुरक्षा प्रयासों को लागू करना, व्यक्तिगत जानकारी के नियंत्रक को सलाह देना और नियंत्रक के समर्थन से पहले किसी भी उप-प्रोसेसर को कनेक्ट न करना शामिल है।

उप-प्रोसेसर

मैं इस अवसर पर अपनी तैयारी से होने वाले किसी भी नुकसान के लिए जिम्मेदार हो सकता हूं कि मैंने अपनी वैध प्रतिबद्धताओं का पालन नहीं किया है और उस स्थिति में जब मैंने नियंत्रकों के निर्देशों का पालन करने में उपेक्षा की है। प्रोसेसर के प्रति मेरे दायित्व नियंत्रक के प्रति प्रोसेसर के कर्तव्यों की तरह हैं।

व्यक्ति' अधिकार

संरक्षण कानूनों के पीछे का बिंदु व्यक्ति को सशक्त बनाना और उन्हें अपनी व्यक्तिगत जानकारी पर नियंत्रण देना है। अधिकांश डेटा गोपनीयता कानून व्यक्तियों की सुरक्षा से संबंधित 'डेटा विषय अधिकारों' के रूप में आम तौर पर बताए गए व्यक्तिगत डेटा से परिचित हैं। यह ध्यान रखना अनिवार्य है कि ये सभी अधिकार 'निरपेक्ष' नहीं हैं, जिसका अर्थ है कि कुछ केवल स्पष्ट परिस्थितियों में लागू होते हैं।

अधिकार

- ✶ व्यक्तिगत जानकारी तक पहुँचने के लिए: व्यक्तियों को अपनी जानकारी के डुप्लिकेट तक पहुँचने और माँग करने का विशेषाधिकार सुरक्षित है।
- ✶ ऑटो-डायनामिक और प्रोफाइलिंग से संबंधित: व्यक्ति मशीनीकृत और यांत्रिक हैंडलिंग के आधार पर उनके बारे में चुने गए विकल्पों का विरोध कर सकते हैं।
- ✶ आपत्ति करना: व्यक्ति किसी संगठन द्वारा अपनी व्यक्तिगत जानकारी के प्रसंस्करण पर आपत्ति कर सकते हैं।
- ✶ व्यक्तिगत जानकारी स्थानांतरित करने के लिए: व्यक्ति समन्वित, आमतौर पर उपयोग किए जाने वाले मशीन-स्पष्ट संरचना प्रारूप में डेटा प्राप्त कर सकते हैं।
- ✶ व्यक्तिगत जानकारी को संबोधित करने के लिए: यदि गलत है तो व्यक्ति अपनी जानकारी को सही कर सकते हैं, या यदि कोई अधूरी है तो उसे पूरा कर सकते हैं।

[5] वही

- ✶ मिटाने के लिए: व्यक्ति अपनी व्यक्तिगत जानकारी तुरंत हटा सकते हैं।
- ✶ व्यक्तिगत डेटा प्रोसेसिंग को सीमित करने के लिए: व्यक्तियों को अपनी व्यक्तिगत जानकारी के प्रसंस्करण पर प्रतिबंध का अनुरोध करने का अधिकार है।

व्यक्तिगत डेटा का प्रसंस्करण

सभी सूचनाओं को कानून के अनुसार संसाधित किया जाना चाहिए। संगठनों के पास प्रसंस्करण के लिए नीचे दिए गए वैध वैध आधारों में से एक होना चाहिए:

- ✶ सहमति: व्यक्ति की अपनी जानकारी को संभालने के लिए।
- ✶ वैध हित: एसोसिएशन या बाहरी लोगों का।
- ✶ संविदात्मक आवश्यकता: किसी समझौते पर जाने या उसे क्रियान्वित करने के लिए प्रबंधन की आवश्यकता होती है।
- ✶ कानूनी प्रतिबद्धता: जिसके लिए एसोसिएशन व्यक्तिगत जानकारी से निपटने के लिए बाध्य है।
- ✶ महत्वपूर्ण रुचि: लोगों की, जहां उनके जीवन को सुनिश्चित करने के लिए संभालना महत्वपूर्ण है।
- ✶ सार्वजनिक हित: आधिकारिक शक्ति का अभ्यास करने वाले या सार्वजनिक हित में कार्य करने वाले संघों के लिए स्पष्ट।

डेटा गोपनीयता कानून संवेदनशील और आपराधिक जानकारी के प्रसंस्करण के लिए विभिन्न स्थितियों का संकेत देते हैं। संवेदनशील जानकारी को आम तौर पर केवल व्यक्ति की स्पष्ट सहमति से ही नियंत्रित किया जा सकता है, सिवाय इसके कि यदि जानकारी वैध जारी रखने या दावों के दस्तावेजीकरण के लिए आवश्यक हो, या यदि कोई वैध, सार्वजनिक हित या प्रशासनिक शर्त हो। भावनाओं और आपराधिक अपराधों से जुड़ी व्यक्तिगत जानकारी आम तौर पर तब तक तैयार की जा सकती है जब तक कि यह किसी विशिष्ट सरकारी प्राधिकरण से प्रभावित होकर या पड़ोस के कानूनों के अनुसार पूरी हो जाती है

भारत में डेटा गोपनीयता पर कानून

सूचना प्रौद्योगिकी अधिनियम, 2000 (संशोधन अधिनियम 2008)

- ✶ **धारा 43A : डेटा की सुरक्षा में विफलता के लिए मुआवजा**

आईटी अधिनियम, 2000 की धारा 43 A के तहत, यह स्पष्ट रूप से कहा गया है कि कोई भी कॉर्पोरेट जो किसी भी डेटा को रखता है या संभालता है जो प्रकृति में संवेदनशील है या किसी भी जानकारी में निहित है और अपने कंप्यूटर संसाधन में नियंत्रण में है, सुरक्षा प्रक्रियाओं को प्रदान करने में तर्कसंगत देखभाल को बनाए रखने और लागू करने में लापरवाही करता है जो किसी भी तरह का नुकसान होता है ऐसे कॉर्पोरेट मुआवजे का भुगतान करने के लिए उत्तरदायी होंगे।

✶ **धारा 65: कंप्यूटर स्रोत दस्तावेजों के साथ छेड़छाड़**

धारा 65 के अनुसार यदि कोई व्यक्ति जानबूझकर कंप्यूटर सिस्टम, कंप्यूटर प्रोग्राम या उसके नेटवर्क के साथ छिपता है, नुकसान पहुंचाता है या संशोधित करता है या जानबूझकर किसी और को ऐसा करने के लिए मजबूर करता है, जब कंप्यूटर स्रोत कोड को बनाए रखने के लिए कानून द्वारा दायित्व होता है तो उसे दंडित किया जाएगा। कारावास जो तीन साल तक हो सकता है, या दो लाख रुपये तक का जुर्माना या दोनों हो सकता है।

✶ **धारा 66: कंप्यूटर से संबंधित अपराध**

धारा 66 में कहा गया है कि यदि कोई व्यक्ति धोखाधड़ी से किसी ऐसे कार्य में लिप्त होता है जो धारा 43 में निर्दिष्ट है, तो उसे तीन साल तक की कैद या जुर्माना जो पांच लाख रुपये तक हो सकता है या दोनों से दंडित किया जाएगा।

✶ **धारा 66 C : पहचान की चोरी के लिए सजा**

धारा 66 C के अनुसार यदि कोई व्यक्ति जानबूझकर और बेईमानी से किसी व्यक्ति के विशिष्ट पहचान विवरण की प्रतिलिपि बनाने और उपयोग करने की कोशिश करता है, उदाहरण के लिए पासवर्ड या डिजिटल हस्ताक्षर, तीन साल तक की कैद और जुर्माना हो सकता है जो एक लाख रुपये तक हो सकता है।

✶ **धारा 69 : किसी भी कंप्यूटर संसाधन के माध्यम से किसी भी जानकारी के अवरोधन या निगरानी या डिक्रिप्शन के लिए निर्देश जारी करने की शक्तियां।**

अधिनियम की धारा 69, उपयुक्त सरकार को किसी भी कंप्यूटर सिस्टम में उत्पन्न, संग्रहीत या प्रसारित होने वाली किसी भी जानकारी को इंटरसेप्ट या डिक्रिप्ट करने का निर्देश देती है। इसका मतलब है कि सरकार को किसी भी कंप्यूटर संसाधन से कोई भी जानकारी एकत्र करने का अधिकार दिया गया है यदि यह पाया जाता है कि ऐसी जानकारी राष्ट्रीय गति और सुरक्षा को परेशान कर सकती है या किसी कानून का उल्लंघन कर सकती है।

✶ **धारा 69 A : किसी कंप्यूटर संसाधन के माध्यम से किसी सूचना की सार्वजनिक पहुंच के लिए अवरोध के लिए निदेश जारी करने की शक्ति**

(1) जहां केन्द्रीय सरकार या उसके द्वारा इस निमित्त विशेष रूप से प्राधिकृत उसके किसी अधिकारी का यह समाधान हो जाता है कि भारत की संप्रभुता और अखंडता, भारत की रक्षा, राज्य की सुरक्षा, विदेशी राज्यों के साथ मैत्रीपूर्ण संबंध या लोक व्यवस्था के हित में या उपरोक्त से संबंधित किसी संज्ञेय अपराध के किए जाने के लिए उद्दीपन को रोकने के लिए ऐसा करना आवश्यक या समीचीन है यह लिखित रूप में दर्ज किए जाने वाले कारणों के लिए उप-धाराओं (2) के प्रावधानों के अधीन हो सकता है, आदेश द्वारा सरकार या मध्यस्थ की किसी भी एजेंसी को जनता द्वारा पहुंच को अवरुद्ध करने या उत्पन्न किसी भी जानकारी को जनता द्वारा पहुंच के लिए अवरुद्ध करने का निर्देश दे सकता है। किसी भी कंप्यूटर संसाधन में प्रेषित, प्राप्त, संग्रहीत या होस्ट किया गया।

(2) वह प्रक्रिया और सुरक्षा उपाय जिसके अधीन जनता की पहुंच को अवरुद्ध किया जा सकता है, वह निर्धारित किया जाएगा।

(3) मध्यस्थ जो उपधारा (1) के अधीन जारी निदेश का अनुपालन करने में असफल रहता है, वह कारावास से, जिसकी अवधि सात वर्ष तक की हो सकेगी, दंडित किया जाएगा और जुर्माने का भी भागी होगा।

✶ **धारा 72 : गोपनीयता और निजता का उल्लंघन**

धारा 72 के अनुसार यदि किसी व्यक्ति ने किसी भी प्रकार के इलेक्ट्रॉनिक रिकॉर्ड जैसे रजिस्टर, पुस्तक आदि तक पहुंच प्राप्त कर ली है और मालिक की सहमति या ज्ञान के बिना ऐसे इलेक्ट्रॉनिक रिकॉर्ड की जानकारी का खुलासा किया है तो उसको दो साल की अवधि तक की कैद, या एक लाख रुपये तक का जुर्माना, या दोनों।

✶ **धारा 72 A : वैध अनुबंध के उल्लंघन में जानकारी के प्रकटीकरण के लिए सजा**

धारा 72 A बिचौलियों पर यह बाध्यता लाती है कि जब कोई सूचना विधि द्वारा निदेशों के अनुसार और स्वामी की सहमति के बिना संगृहीत की जाती है, जानबूझकर विधिविरुद्ध प्रयोजन के लिए प्रयोग की जाती है तो तीन वर्ष तक कारावास, या पांच लाख रुपए तक जुर्माना, या दोनों से दंडनीय होगा।

अन्य देशों में डेटा सुरक्षा

डेटा संरक्षण पर भारतीय कानून और विकसित देशों के कानूनों की तुलना में भारतीय कानून द्वारा आवश्यक उचित शर्त को सूचीबद्ध किया जा सकता है। डेटा संरक्षण अधिनियम, 1998, यूनाइटेड किंगडम में उपलब्ध है। डेटा संरक्षण अधिनियम मूल रूप से यूनाइटेड किंगडम में लोगों की विशिष्ट जानकारी को गोपनीयता के साथ-साथ सुरक्षा प्रदान करने के लिए स्थापित किया गया है। दिए गए अधिनियम के अनुसार, एक व्यक्ति या कंपनी जो व्यक्ति की जानकारी एकत्र करती है, उसे सूचना आयुक्त के साथ पंजीकरण करना चाहिए, जिसे अधिनियम की निगरानी के लिए सार्वजनिक प्राधिकरण के अधिकारी के रूप में प्रत्यायोजित किया गया है यह अधिनियम जानकारी के संग्रह पर कुछ प्रतिबंध प्रदान करता है। इस प्रकार एकत्र की गई किसी व्यक्ति की जानकारी संतोषजनक, लागू होगी और उस वस्तु के अनुसार नहीं बढ़ाई जाएगी जिसके लिए उन्हें संभाला गया है।

संयुक्त राज्य अमेरिका और यूरोपीय संघ दोनों यूरोपीय संघ की तुलना में अपने निवासियों के सुरक्षा आश्वासन को उन्नत करने पर जोर देते हैं। अमेरिका सुरक्षा की एक वैकल्पिक रणनीति अपनाता है। संयुक्त राज्य अमेरिका ने क्षेत्रीय पद्धति को शामिल किया जो कानूनों, दिशानिर्देशों और अन्य स्व-विनियमों में मिश्रणों पर निर्भर करती है। संयुक्त राज्य अमेरिका में, जानकारी आमतौर पर कुछ वर्गों में एकत्रित की जाती है जो उनकी उपयोगिता और महत्व पर आधारित होती है। वहां से, इसी तरह सूचना के विभिन्न वर्गों को वैकल्पिक स्तर की सुरक्षा प्रदान की जाती है। जबकि आईटी अधिनियम सूचना के निष्कर्षण, सूचना के विनाश आदि का प्रबंधन करता है, संगठनों को सूचना की पूर्ण सुरक्षा नहीं मिल सकती है जिसके माध्यम से वे अंततः जानकारी को सुरक्षित रखने के लिए अलग-अलग निजी समझौतों में जाने के लिए बाध्य होते हैं। ऐसे समझौतों में समग्र समझौते के समान ही लागू करने योग्य प्रक्रिया होगी।

यूरोपीय संघ ने अपने देश के सभी सदस्यों को व्यक्तिगत डेटा की सुरक्षा पर एक व्यापक निर्देश अधिकृत किया है। अमेरिका और यूरोपीय संघ ने सेफ हार्बर समझौते के माध्यम से मिलकर काम करने पर सहमति व्यक्त की है। भारतीय भी समझदारी से काम लेंगे और यूरोपीय संघ के जनादेश पर सहमत होंगे, क्योंकि इसमें एक बंडल भी है।

सूचना बीमा कानून को एक अलग नियंत्रण के रूप में रखने के लिए किए जा रहे प्रयासों के बावजूद, 2006 के बिल में कुछ खामियां हैं। बिल का मसौदा तैयार करना यूनाइटेड किंगडम के डेटा संरक्षण अधिनियम के आधार पर तैयार किया गया है जबकि वर्तमान आवश्यकता एक व्यापक अधिनियम की है इन पंक्तियों के साथ यह प्रस्तावित किया जाता है कि सूचना बीमा के साथ पहचान करने वाले अमेरिकी कानूनों के आधार पर एकत्रित मसौदा आज की आवश्यकता के लिए अधिक महान होगा। भारतीय कानून की वास्तविक आवश्यकता की जांच भारत के कानूनों की विकसित देशों के कानूनों से तुलना करने पर की जा सकती है। यूके का डेटा संरक्षण अधिनियम, १९९८ मूल रूप से यूके में लोगों की व्यक्तिगत जानकारी की सुरक्षा और संरक्षण देने के लिए शुरू किया गया है।

निष्कर्ष

यह सही समय है कि भारत के पास डेटा संरक्षण कानूनों पर अपना कानून होना चाहिए जो सूचना के विशेषाधिकार सुनिश्चित करेगा जो एकत्र किए गए डेटा के उपयोग को प्रतिबंधित करेगा और इस तरह के अन्य उद्देश्यों के लिए एकत्र की गई जानकारी के अलावा जिसके लिए इसे एकत्र किया गया था। 2000 के आईटी अधिनियम को डेटा गोपनीयता या सूचना संरक्षण कानून नहीं माना जा सकता है। अधिनियम में कोई विशेष सूचना गोपनीयता या सुरक्षा मानक शामिल नहीं हैं। आईटी अधिनियम, 2000 का दायरा गैर-विशिष्ट है क्योंकि यह ई-गवर्नेंस, इलेक्ट्रॉनिक हस्ताक्षर, प्रमुख बुनियादी ढांचे और साइबर अपराधों पर केंद्रित है। आईटी अधिनियम, 2000 की तुलना ऊपर चर्चा किए गए अन्य विकसित देशों के कानूनों से करना पर्याप्त नहीं होगा। भारत में डेटा संरक्षण कानून पर विशिष्ट कानूनों की कमी है, जो अपने नागरिकों की गोपनीयता पर पुनर्विचार करने के लिए बहुत प्रभावित है। यूरोपीय संघ और अमेरिका के ग्राहकों को पूर्ण सुरक्षा आदेश के साथ सुनिश्चित किया जाता है, और आंशिक रूप से यह आवश्यक है कि सुरक्षा की आवश्यकता संगठनों पर डाली जाए, न कि किसी व्यक्ति के डेटा को उन देशों में स्थानांतरित किया जाए जो पर्याप्त आश्वासन पर सौदेबाजी करते हैं। नतीजा यह है कि यूरोपीय ट्रेड यूनियनों ने सूचना बीमा को एक ऐसे मुद्दे के रूप में संदर्भित किया है जिस पर कई वैश्विक आउट-सोर्सिंग सौदेबाजी में विचार किया जाना चाहिए। इसके उच्च समय भारत को संवेदनशील जानकारी संग्रहीत करने और प्रसारित करने के लिए अन्य विकसित देशों की तुलना में डेटा संरक्षण पर एक व्यापक कानून की आवश्यकता है।

संदर्भ सूची

1. फिल मेनी, रिचर्ड चुडज़िनस्की, 2020 , डेटा गोपनीयता हैंडबुक - डेटा गोपनीयता अनुपालन के लिए एक स्टार्टर गाइड। ।

2. सूचना प्रौद्योगिकी अधिनियम, 2000 (संशोधन अधिनियम 2008)

3. पीटर कैरी, 2020 , डेटा संरक्षण-यूके कानून के लिए एक व्यावहारिक मार्गदर्शिका।

4. एलिफ़ किसो कॉर्टेज़, 2021, एक्शन 5 में दुनिया भर में डेटा संरक्षण गोपनीयता कानून। डैनियल जे। सोलोव, पॉल एम। श्वार्ट्ज, 2020, उपभोक्ता गोपनीयता और डेटा संरक्षण, तीसरा संस्करण।

6. ली एंड्रयू बायग्रेव, 2014, डेटा गोपनीयता कानून: एक अंतर्राष्ट्रीय परिप्रेक्ष्य, ऑक्सफोर्ड छात्रवृत्ति ऑनलाइन, आईएसबीएन-13: 9780199675555