खण्ड-9, अंक-1, वर्ष-2021, मु0प्र0 134-138
D.O.I.: https://doi.org/10.22445/avsp.v9i1.25
SJIF (2021) : 7.247

डाटा लीक के बढ़ते मामले एवं विधि

दीपायन मालवीय
एकेडेमिक ट्यूटर एण्ड ट्रिप फैलो
ओ0 पी0 जिंदल यूनिवर्सिटी, सोनीपत–131 001, हरयाणा, भारत
dmalaviya@jgu.edu.in

प्राप्ति तिथि–14.06.2021, स्वीकृति तिथि–08.09.2021

सार– डाटा नई मुद्रा है और जिसके पास डाटा है उसके पास बाजारों को नियंत्रित करने की क्षमता है। प्रत्येक वस्तु की तरह, डाटा को कई तरीकों से प्राप्त किया जा सकता है। कुछ तरीके वैध हैं और अन्य अवैध। अर्थव्यवस्थाओं के डिजिटलीकरण के साथ डाटा भी अब डिजिटल रूप में संग्रहीत किया जा रहा है। इसने डाटा के भंडारण को सुविधाजनक बना दिया है, लेकिन डाटा लीक और डाटा चोरी की घटनाओं में भी वृद्धि हुई है। यह लेखन उन बिंदुओं को संबोधित करना चाहता है जिन पर डाटा की सुरक्षा सबसे कमजोर है और सुरक्षा की आवश्यकता है। इतना ही नहीं, इस लेख के माध्यम से यह भी पता लगाने की कोशिश की जाएगी कि डाटा लीक की बढ़ती समस्या को रोकने के लिए कानून पर्याप्त हैं या नहीं। और अगर पर्याप्त नहीं है तो डाटा लीक होने की स्थिति में एक पीड़ित किस प्राधिकार की सहायता ले कर भारमुक्त हो सकता है। और यदि नहीं तो कानून व्यवस्था में किस तरह की बदलाव की आवश्यकता है।

बीज शब्द– डाटा, डाटा लीक, साइबर सुरक्षा, सूचना प्रौद्योगिकी कानून, डाटा सुरक्षा कानून

Rising cases of Data Leaks and the Law

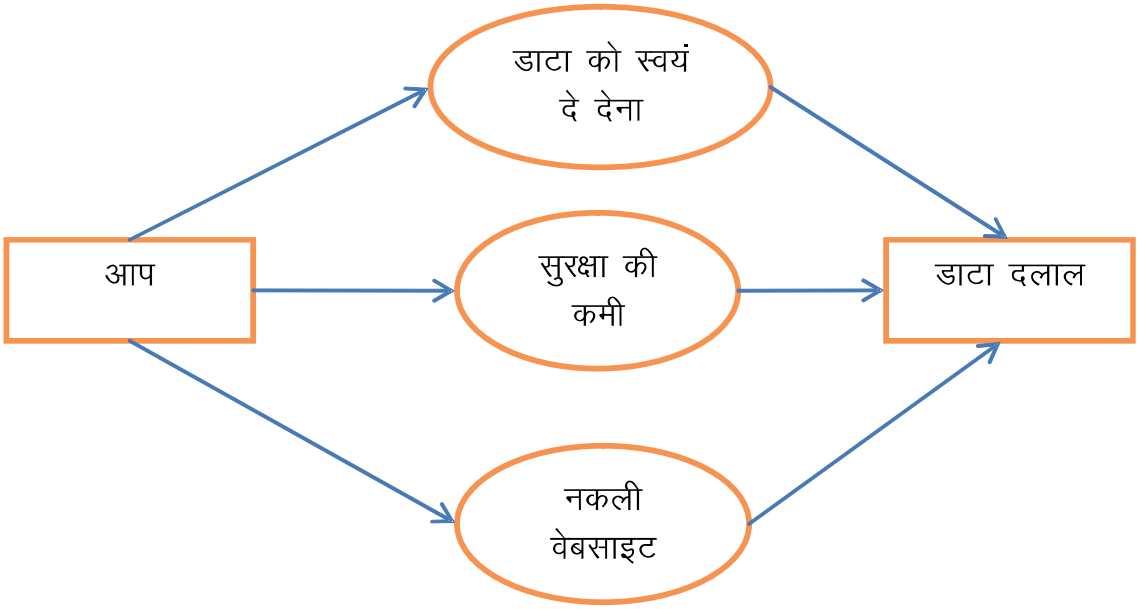
Deepayan Malaviya
Academic Tutor &TRIP Fellow
O. P. Jindal Global University, Sonipat-131 001, Haryana, India
dmalaviya@jgu.edu.in

Abstract- Data is the new asset and whoever has the data has the ability to control the markets. Just like everything else, data tool can be obtained in numerous ways. Some ways are legilitame and others are illegitmate. With the digitization of economies data is also now being stored in digitial form. This has made the storage of data convenient but has also increased the instances of data leak and data theft. The paper seeks to address the points at which data is most vulnerable and needs protection. Not only this, the paper also seeks to ascertain whether the laws are adequate to curb the rising problem of data leak or not.It also embodies the options available to the victim which can be utilized to reduce the damage caused by such leak. The paper would further suggest ways in which the law can be modernized to tackle the rising problem of data leaks.

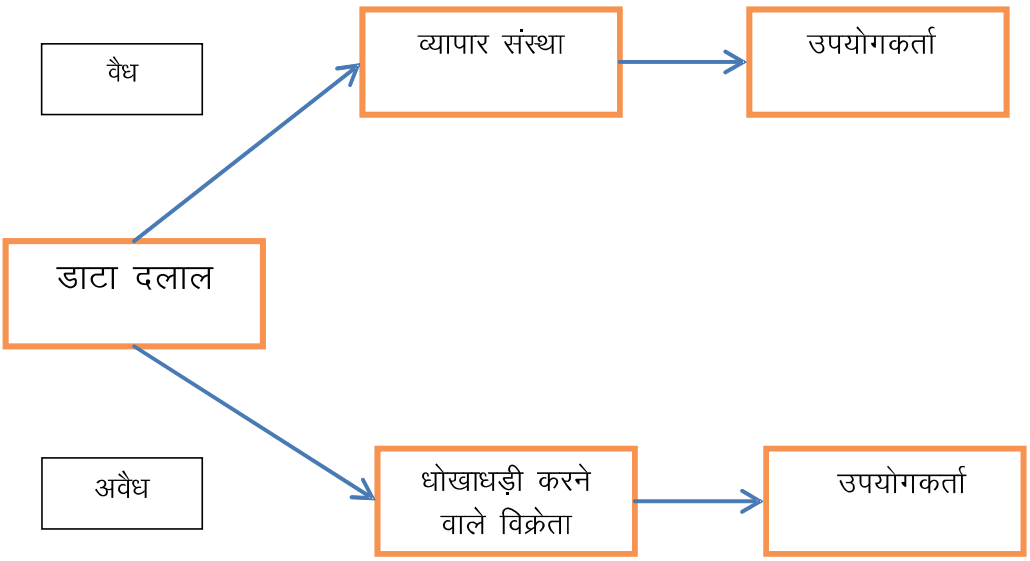
Key words- data, data leak, cyber security, information technology law, data protection law

१. परिचय– आज सूचना प्रौद्योगिकी काल में कहा जा रहा है कि डाटा ही अर्थव्यवस्था की जड़ है और जिसके पास डाटा है वो ही अर्थव्यवस्था को नियंत्रित कर सकता है। इसके चलते डाटा को प्राप्त करने के लिए बहुत सारे तरीके अपनाए जाते है इनमें से कई तरीके वैध है तो कई अवैध। एक तरफ तो भारतीय संविधान अन्नुछेद २१ के अंतर्गत गोपनीयता का अधिकार प्रदान करता है[1] परन्तु दूसरी तरफ हमें देखने को मिलता है की स्पाइवेयर ऐप्स को आसानी से खरीदा और बेचा जा सकता है।[2] अगस्त २०२० में गूगल ने इन एप्पस पर डाउनलोड पर रोक तो लगाई परन्तु भारतीय कानून ऐसी एप्पस के प्रयोग पर कोई रोक नहीं लगता[3] और चौंका देने वाली बात यह है कि दिल्ली उच्च न्यायालय ने कहा है की निजता के उल्लंघन में एकत्र किए गए साक्ष्य अदालत में अस्वीकार्य नहीं हैं।[4] यह तो हो गई डाटा एकत्रित करने की बात पर देखना अब यह है कि हमारा डाटा हमारे ही विरुद्ध कैसे उपयोग में लाया जाता है और सबसे महत्वपूर्ण बात यह है कि हमारा डाटा धोखाधड़ी करने वाले विक्रेता तक पहुंचता कैसे है। इस परिप्रेक्ष्य में डाटा दलाल, जो कि, आमतौर पर एक कंपनी होती है, डाटा को एकत्रित करती है और फिर मुनाफे के लिए उस डाटा को किसी भी व्यक्तिया कंपनी को बेच देती है। डाटा संग्रहण के मुख्यतः तीन तरीके है। पहला, डाटा को स्वयं दे देना– ऐसा कई बार होता है कि हम अपना डाटा स्वयं देते है परन्तु हमें यह नहीं पता होता कि डाटा का उपयोग किस तरह किया जायेगा, दूसरा, कई बार सुरक्षा की कमी के कारण डाटा लीक हो जाता है और धोखाधड़ी करने वाले विक्रेता तक पहुँच जाता है, तीसरा, धोखाधड़ी करने वाले विक्रेता ही नकली वेबसाइट बना कर डाटा प्राप्त कर लेते हैं। पहले बिंदु के परिप्रेक्ष्य में कंपनी की गोपनीयता नीति एक अहम भूमिका निभाती है। गोपनीयता नीति में लिखा होता है कि कंपनी एकत्रित किया हुआ

डाटा तृतीय पक्ष के साथ साझा करेंगे। इसका परिणाम यह होता है कि जब हम किसी प्रतिपुष्टी फार्म या अन्य फार्म को सहमति देते हैं तो हम स्वयं अपना डाटा उन तृतीय पक्षों को सौप देते हैं। एक बार कंपनी तक यह डाटा पहुँच जाता है तो उस डाटा का मुख्यतः दो तरह से उपयोग होता है। पहला विपणन, दूसरा धोखाधड़ी।



उपर्युक्त चर्चा से यह स्पष्ट हो जाता है कि भारतीय नागरिक को यह नहीं पता है की उसका डाटा किन तरीको से संग्रहीत करा जा सकता है एवं डाटा का उपयोग किस तरह से किया जा सकता है। इन चुनौतियों से निपटने के लिए भारत सरकार ने व्यक्तिगत डाटा सुरक्षा बिल, २०१६ को संसद मे पेश किया।[5] इस बिल के माध्यम से अब कंपनियों को डाटा साझा करने से पहले ग्राहकों से स्पष्ट सहमति लेनी होगी। ग्राहकों को यह भी बताना होगा कि उनके द्वारा दिये गए डाटा का उपयोग कैसे किया जायेगा और स्थिति से प्रस्थान के मामले में ग्राहक के पास ये शक्ति होगी कि वह अपनी सहमति वापस ले सके। पर दुर्भाग्य से डाटा सुरक्षा बिल, २०१६ अभी कानून नहीं बना है और भारत में सूचना प्रौद्योगिकी अधिनियम–२००० ही डाटा संरक्षण से संबंधित एकमात्र कानून है।[6]



२. **भारत में डाटा संरक्षण की स्थिति–** भारत के संविधान एवं सूचना प्रौद्योगिकी अधिनियम, २००० की धारा ४३ ए के अनुसार व्यक्तिगत डाटा की सुरक्षा के लिए डाटा प्रत्ययी कानूनी रूप से बाध्य हैं। परन्तु हाल ही में हुए डाटा उल्लंघनों के कारण सैकड़ो सरकारी अधिकारियो के व्यक्तिगत विवरण, यथा उनके मोबाइल नंबर, ईमेल अड्रेस, आधार नंबर, पैन नंबर बैंक खाता संख्या अथवा अन्य संवेदनशील जानकारी लीक हो गई है।[7] परन्तु सवाल ये उठता है कि जब धारा ४३ ए है तो डाटा लीक होने पर कोई अधिसूचना क्यों नहीं दी जाती ? इस सवाल के जवाब के लिए हमें धारा ४३ ए का गहन अध्ययन करने की आवश्यकता है। धारा ४३ ए हमें बताती है की संवेदनशील जानकारी लीक के लिए ही मुआवजा देने के लिए बाध्य होगी। पर सवाल अब यह उठता है की संवेदनशील जानकारी क्या है? इसके लिए हमें सूचना प्रौद्योगिकी (उचित सुरक्षा व्यवहार और प्रक्रियाएं और संवेदनशील व्यक्तिगत डेटा या सूचना) नियम, २०११ का अध्ययन करना पड़ेगा।[8] अध्ययन करने पर हम पाएंगे की यदि आपका नाम, ईमेल, पता या पासपोर्ट भंग हो गया है तो ऐसा कोई निवारण नहीं है, क्योंकि इसमें से कोई भी संवेदनशील डाटा के रूप में वर्गीकृत है ही नहीं और एक बार यह जानकारी गलत संस्था के पास पहुँच जाती है तो प्रारम्भ होता है कपटपूर्ण कॉल और ईमेल का सिलसिला। इसके चलते भारत में डाटा संरक्षण में बहुत कमियां है और इन कमियों के कारण अंततः उपयोगकर्ता की ही जिम्मेदारी बनती है।

अभी तक चर्चा हुई है कि नियमों में खामिया होने के कारण घोटालेबाज मासूम लोगों का डाटा प्राप्त करते हैं पर देखना अब ये है कि ये घोटालेबाज इस डाटा का उपयोग कैसे करते हैं। चूंकि फोन नंबर और ईमेल पते को संवेदनशील जानकारी के रूप में वर्गीकृत नहीं किया जाता है, घोटालेबाज इस जानकारी का उपयोग निर्दोष लोगों का विश्वास हासिल करने के लिए करते हैं और एक बार जब यह विश्वास प्राप्त हो जाता है तो घोटालेबाज सीवीवी नंबर और ओटीपी प्राप्त करने के लिए करते है और ये जानकारियाँ प्राप्त करने के लिए भ्रामक रणनीति का उपयोग करते हैं। एक बार घोटालेबाज को सब जानकारी प्राप्त हो जाती है तो वित्तीय धोखाधड़ी परिणाम होता है। कहने का तात्पर्य ये है कि यह समस्या दो तरफा है और प्रमुख रूप से कानून में कमी होने की वजह से ये सारी समस्याएँ और भी बढ़ जाती हैं।

३. ऑनलाइन धोखाधड़ी के मामले में उपाय– जैसे ही आपको पता चले कि आपके क्रेडिट/डेबिट कार्ड से कोई संदिग्ध लेनदेन हुआ है, कार्ड जारीकर्ता को तुरंत सूचित करें। बैंक में औपचारिक शिकायत दर्ज करानी चाहिए और आदर्श रूप से कार्ड या खाते को तुरंत ब्लॉक करने के लिए कस्टमर केयर नंबर पर कॉल करनी चाहिए। एक बार कार्ड जारीकर्ता या बैंक को धोखाधड़ी वाले लेनदेन के बारे में सूचित कर दिया गया है, तो किसी को निकटतम पुलिस स्टेशन में लिखित शिकायत दर्ज करनी चाहिए। परन्तु अभ्यास से पता चलता है कि पुलिस अक्सर केस दर्ज करने से मना कर देती है। ऐसे में किसी भी न्यायालय में दस्तक दी जा सकती है और आपराधिक प्रक्रिया संहिता, १९७३ धारा १५६(३) के तहत पुलिस को निर्देश देने की प्रार्थना की जा सकती है। ऐसा भी देखने को मिलता है की पुलिस शिकायतकर्ता को साइबर सेल में रिपोर्ट पंजीकृत कराने का निर्देश दे देती है। ऐसी स्थिति में शिकायतकर्ता के पास दो विकल्प होते हैं। पहला, साइबर सेल में जाकर शिकायत दर्ज कराएं, दूसरा, प्रभारी पुलिस अधिकारी से शिकायत दर्ज करने और साइबर सेल को फॉरवर्ड करने का अनुरोध करें।

शिकायत दर्ज हो जाने के बाद सवाल यह उठता है कि क्या बैंक के ग्राहक को उसके पैसे वापस मिलेंगे या नहीं ? इसके लिए प्राविधान यह कहता है कि यदि धोखाधड़ी होती है और बैंक की गलती नहीं है और यह किसी तीसरे पक्ष द्वारा धोखाधड़ी, फिशिंग आदि के माध्यम से किया गया था, तो आरबीआई के नियम के तहत यदि उल्लंघन की सूचना तीन दिनों के अंदर दी गई है तो ग्राहक को कुछ कीमत अदा नहीं करनी होगी, परन्तु फर्जी लेनदेन की सूचना सात दिनों के बाद दी जाती है तो ग्राहक की प्रति लेनदेन देयता लेनदेन मूल्य या केंद्रीय बैंक द्वारा निर्धारित राशि, जो भी कम हो, तक सीमित होगी। परन्तु शिकायत दर्ज करना और पैसे वापस ले लेना कोई स्थायी समाधान नहीं है। स्थायी समाधान तो होगा कानून को सशक्त बनाना और ऑनलाइन धोखेबाजी को जड़ से समाप्त करना।[9]

४. कानूनी ढांचे की सीमाएं– सूचना प्रौद्योगिकी अधिनियम–२००० डाटा न्यासियों पर कुछ दायित्वों को लागू करता है परन्तु ये दायित्व कोई ठोस निवारण तंत्र प्रदान नहीं करता। ऐसा होने के निम्नलिखित कारण हो सकते हैं–

४.१ सूचित करने की कोई बाध्यता नहीं– उल्लंघन होने की स्थिति में प्रभावित उपयोगकर्ताओं को सूचित करने के लिए डाटा न्यासियों पर कोई कानूनी दायित्व नहीं है। संचार–अनुपालन–जांच एक तीन–चरणीय प्रक्रिया है जिसका उल्लंघनों के प्रभाव को कम करने के लिए पालन किया जाना चाहिए। इसका मतलब यह है कि डाटा उल्लंघन होने पर डाटा न्यासियों को जनता को सूचित करना चाहिए। परन्तु यह मानक संचालन प्रक्रिया का पालन हमें देखने को नहीं मिलता।

४.२ संवेदनशील व्यक्तिगत डाटा को संकीर्ण रूप से परिभाषित किया गया है– धारा ४३ ए केवल संवेदनशील डाटा के लापरवाही से संचालन के लिए क्षतिपूर्ति प्रदान करती है। २०११ के नियमों के नियम ३ के अनुसार, संवेदनशील डाटा पासवर्ड, वित्तीय जानकारी, यौन अभिविन्यास, चिकित्सा रिकॉर्ड और बायोमेट्रिक जानकारी जैसी जानकारी तक सीमित है। नाम, ईमेल पता, घर का पता और पासपोर्ट विवरण जैसी जानकारी का उल्लंघन होने पर आईटी अधिनियम, २००० कोई निवारण प्रदान नहीं करता है। ऐसा न होने से ऑनलाइन घोटाला को सहयोग मिलता है।

४.३ जांच का अभाव– जब उल्लंघन होते हैं, तो उपयोगकर्ताओं को आईटी अधिनियम, २००० की धारा ४३ ए के तहत मुआवजे का दावा करने में सक्षम बनाने के लिए उचित जांच नहीं की जाती है।

४.४ अपर्याप्त निवारण तंत्र– आईटी अधिनियम की धारा ४६ के तहत निवारण तंत्र अपर्याप्त है। ऐसा इसलिए क्योंकि जिन मामलो में

डाटा सरकार की हिरासत में होता है उन मामलो में न्यायनिर्णायक अधिकारी विवाद का निर्णय नहीं कर सकते। ऐसा इसलिए है क्योंकि उन्हें सरकार ही नियुक्त करती है और इस कारण से सरकार से जुड़े विवाद को हल करने के लिए आवश्यक रूप से स्वतंत्रता नहीं होती है।

५. कानूनी व्यस्था में सुधार की आवश्यकता– उपरोक्त चर्चा से यह पता लगाया जा सकता है कि आज हम जिस समस्या का सामना कर रहे हैं वह दो आयामी है। एक ओर उपयोगकर्ता को कीमती डाटा खोने का प्रत्यक्ष जोखिम होता है और दूसरी ओर उपयोगकर्ता के डेटा को संग्रहीत करने वाले प्रत्ययी को साइबर हमलों का खतरा होता है जो इस डाटा को चोरी करने के लिए निर्देशित होते हैं। और हाल की प्रथाओं से पता चलता है कि साइबर हमले बढ़ रहे हैं और उपयोगकर्ता के डाटा के लिए भी खतरा बढ़ गया है। ऐसा कहा जा रहा है कि भारतीय कानूनी ढांचा दो आयामी समस्या से निपटने के लिए अपर्याप्त है। इस प्रकार, इसमें सुधार की आवश्यकता है ताकि उपयोगकर्ता की गोपनीयता की रक्षा की जा सके। ऐसी परिस्तिथियों में कहा जा सकता है की हल भी दो आयामी होना चाहिए।

५.१ उपयोगकर्ताओं के लिए दिशा–निर्देश–

५.१.१ जागरूकता अभियान– दिल्ली में किए गए एक सर्वेक्षण से पता चला है कि ७५ % उत्तरदाताओं ने अपने व्यक्तिगत विवरण साझा करने से पहले गोपनीयता नीति को कभी नहीं पढ़ा। गोपनीयता नीति को पढ़ना निस्संदेह महत्वपूर्ण है, लेकिन हम में से बहुत से लोग यह भी नहीं जानते हैं कि गोपनीयता नीति क्या है। यह उपयोगकर्ताओं की घोर अज्ञानता और इस तरह की अज्ञानता से जुड़े खतरे को दर्शाता है। ये दर्शाता है कि उपयोगकर्ता को कानून से अधिक जागरूकता की आवश्यकता है। एक बार अगर उपयोगकर्ता जागरूक हो गए तो वह अपना डाटा सोच समझ कर साझा करेंगे।

५.१.२ डाटा साझा करने के प्रति सावधान रहें– हम में से बहुत से लोग नहीं जानते कि पब्लिक हॉटस्पॉट का इस्तेमाल करने से डाटा लीक होने का खतरा कई गुना बढ़ जाता है। हम में से बहुत से लोग यह भी नहीं जानते हैं कि फीडबैक फॉर्म में ऐसी जानकारी होगी जिसे ऑनलाइन खरीदा और बेचा जा सकता है और इसका दुरुपयोग भी किया जा सकता है। इसलिए साझा शेयर करने में सावधानी बरतना बहुत जरूरी है।

५.२ डाटा न्यासियोंके लिए दिशा–निर्देश– डाटा न्यासियों द्वारा कानून के संभावित उल्लंघन को ध्यान में रखते हुए, यह ज्ञात किया जा सकता है कि कानून में खामियां होने की वजह से न्यासिया कानून का उल्लंघन करती है। इसको ध्यान में रखते हुए सरकार को निम्नलिखित सिफारिशों पर अमल करना चाहिए–

- पिछले दो वर्षों में जिन डाटा न्यासियों में डाटा के परिपेक्ष में उल्लंघनों का अनुभव हुआ है, उन न्यासियों के आचरण की जांच हो ।
- डाटा के लीक का अनुभव होने पर उपयोगकर्ताओं को सूचित करने के लिए डाटा न्यासियों को कर्तव्य परायण बनने के आदेश दिए जाय।
- सुनिश्चित करें कि डाटा लीक से प्रभावित भारतीय नागरिकों को पर्याप्त मुआवजा प्रदान किया जाता है।
- सूचना प्रौद्योगिकी अधिनियम–२००० में उपयुक्त परिवर्तन करने के लिए कदम उठाना आवश्यक है जिससे एक न्यायिक अधिकारी को धारा ४६ के तहत विवादों का न्याय करने का अधिकार प्राप्त हो।
- निजी संस्थाओं की तुलना में सरकार और सरकार के स्वामित्व वाली संस्थाओं को सख्त डाटा सुरक्षा मानकों पर पकड़ें।
- सूचना प्रौद्योगिकी (उचित सुरक्षा प्रथाओं और प्रक्रियाओं और संवेदनशील व्यक्तिगत डेटा या सूचना) नियम, २०११ के नियम ३ में उल्लिखित व्यक्तिगत रूप से पहचान योग्य जानकारी के प्रकारों को बढ़ाएं, यह देखते हुए कि वर्तमान सेट असाधारण रूप से संकीर्ण है।
- गतिशील अनुपालन तंत्र सुनिश्चित करने के लिए सुरक्षा उपायों के लिए "जवाबदेही लॉग" बनाए रखने की आवश्यकता को अनिवार्य करें।
- भारतीय नेटवर्क और डाटाबेस की सुरक्षा को लागू करने के लिए सम्मिलित डाटा के पैमाने और संवेदनशीलता के आधार पर सुरक्षा अनुपालन की एक स्तरीय प्रणाली का परिचय दें।

६. समापन टिप्पणी– हर वह दिन जो बिना डाटा संरक्षण कानून के गुजरता है भारतीय नागरिक के गोपनीयता के अधिकार को हानि पहुँचता है। उपरोक्त शोध से ये साफ हो जाता है की समस्या दो स्तरीय है। पहले स्तर में नागरिक से डाटा चुराया जाता है दूसरे स्तर में जहाँ पर नागरिक का डाटा संग्रहित है वहीं से डाटा चुरा लिया जाता है। जब समस्या दो स्तरीय है तो उपाय भी दो स्तरीय होना चाहिए। नागरिक से डाटा चोरी होने से बचाने के लिए आवश्यकता है कि व्यक्तिगत डाटा सुरक्षा बिल जल्द से जल्द कानून बने, और डाटा प्रत्ययी से डाटा लीक न हो इसके लिए जरूरत है की प्रौद्योगिकी अधिनियम–२००० में संशोधन किये जाय।

डाटा को सुरक्षित करने के लिए हमें अपनी साइबर स्पेस को सुरक्षित करना पड़ेगा। और इसके लिए आवश्यकता है कि विधि और प्रौद्योगिकी साथ–साथ विकसित हो। वर्ल्ड इकोनॉमिक फोरम की वैश्विक जोखिम रिपोर्ट–२०२१ में कहा गया है, साइबर सुरक्षा की

विफलता अगले दशक में मानवता के सामने सबसे बड़े खतरों में से एक है।[10] इस प्रकार यह आवश्यक है कि हम ऐसी विफलताओं को रोकने के लिए उपयुक्त कदम उठाना शुरू करें और निवारण प्रदान करने के लिए तंत्र विकसित करें।

संदर्भ

1. सुप्रीम कोर्ट ऑफ इंडिया (२०१८) क.एस.पुत्तास्वामी बनाम यूनियन ऑफ इंडिया
2. स्निग्धा, पूनम एवं समर्थ, बंसल (२०२०) रेस्ट ऑफ दी वर्ल्ड, https://restofworld.org/2020/all-the-data-fit-to-sell/
3. सिक्योरिटी मैगजीन (२०२०) सिक्योरिटी मैगजीन, https://www.securitymagazine.com/articles/93394-google-bans-stalkerware-apps-from-the-play-store
4.सिन्हा, भद्रा (२०२०) एविडेंस कलेक्टेड इन ब्रीच ऑफ प्राइवेसी डस नॉट मेक आईटी इनदमिसिबले इन कोटर्स दिल्ली हाई कोर्ट https://theprint.in/judiciary/evidence-collected-in-breach-of-privacy-does-not-make-it-inadmissible-in-court-delhi-hc/452288/
5. मिनिस्ट्री ऑफ लॉ एंड जस्टिस (२०१६) पी. अर. एस लेजिस्लेटिव रिसर्च
https://prsindia.org/billtrack/the-personal-data-protection-bill-2019
6. मिनिस्ट्री ऑफ लॉ एंड जस्टिस (२००६) दी इनफार्मेशन टेक्नोलॉजी एक्ट, २०००
https://legislative.gov.in/sites/default/files/A2000-21_0.pdf
7. सिंह, विजयता जाग्रति चंद्र, (२०२१) डाटा ब्रीच एक्सपोसेस मेल्स, पसवोर्ड्स ऑफ सेवेरल गवर्नमेटन ऑफिशल्स टू हैकर्स
https://www.thehindu.com/news/national/data-breaches-expose-emails-passwords-of-several-government-officials-to-hackers/article34798982.ece?homepage=true
8. मिनिस्ट्री ऑफ इलेक्ट्रॉनिक्स एंड इनफार्मेशन टेक्नोलॉजी, (२०२१) मिनिस्ट्री ऑफ इनफार्मेशन ब्राडकास्टिंग
https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf
9. रिजर्व बैंक ऑफ इंडिया, (२०१७), लायबिलिटी लिमिटिंग ऑफ कस्टमर्स इन अनधिकृत बैंकिंग ट्रांसक्शन्स
https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15D620D2C4D2CA4A33AABC928CA6204B19.PDF
10. वर्ल्ड इकोनॉमिक फोरम (२०१६) दि ग्लोबल रिस्क रिपोर्ट २०२१
http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf