Quest Journals
Journal of Research in Humanities and Social Science
Volume 10 ~ Issue 1 (2022)pp: 84-90
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Digital Globalisation and It's Link With Indian Data Privacy Bill - Effects And Advantages

Shireen Singh

ABSTRACT
Mobility (Geographic Knowledge Discovery, Data Mining, Cloud computing, etc.) advancements in technology carry with them unexpected issues, one of which is the danger to "privacy." In India, there is no comprehensive legislative structure that addresses the problem of privacy. The ITA Act 2008, which was enacted to make e-commerce easier, is a good starting point for dealing with severe cyber concerns. This framework suggests a complete approach to meet Indian privacy needs now and in the future. Digital India is examined as a factor in the Make-in-India initiative for the IT and BPM sector. Digital economy is merging with the digital economy, which is leading to smart cities and e governance. Increased demand for IT gear and the adoption of ICTs will be a result of this. India's digital revolution would be aided by the country's efforts to improve digital literacy. It has been claimed by the Indian government that it intends to eliminate all IT hardware imports by 2020. We could witness a spike in IT gear purchases as a result of the rise in cashless transactions. The government of India has made a number of steps to improve public access to digital information, as detailed in this article. Additionally, some of the most significant roadblocks to digitalization are discussed.

***R**eceived 04 Jan, 2022; **R**evised 13 Jan, 2022; **A**ccepted 15 Jan, 2022 © The author(s) 2022.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

The Indian government is a signatory to a number of international privacy agreements. India's constitution treats the right to privacy as an unstated but essential right. Privacy and data protection laws are not specified in India. A special clause of the Information Technology Act, 2000 (the Act') provides for the protection of electronic data. Both Sections 43A and 72A, which deal with privacy, were introduced to the Information Technology Act of 2000 by the Information Technology Act of 2008.

Many people have the mistaken notion that India's privacy regulations are notoriously lax. However, our understanding of privacy in India is somewhat different from that of the Western nations. If India's Supreme Court rules that India has an implied right to privacy, then the fate of India's data privacy law and its ID-system would be interwoven. A national privacy regulator does not exist in India since the country does not have any such agencies. A Data Protection Authority of India is proposed in the Privacy Bill, which would oversee compliance with the legislation.[1]

Although the Information Technology Act, 2000 (IT Act) has provisions to safeguard personal data, the notion of data protection is still nascent in India. The standardisation of cloud computing's technological characteristics necessitates regulations as well. If the short-term remedy fails, the long-term form of Indian data protection legislation may change.

The Latin word "Privatus," which means "separated from rest," is the source of the term "privacy." In other words, the capacity to hide information about oneself and disclose oneself selectively might be defined as such. To accomplish information security, the protection of the information has been broadened to encompass not only confidentiality but also integrity and availability, due to the advent of new technologies. Data digitization has made data more readily available, but it has also produced chaos due to data overflow, making massive data more difficult to handle. Personal and private information, such as credit card numbers, is also included. Individuals and the country may both suffer harm and losses if this data is handled incorrectly.

[1] Azmi, Ida. (2002). E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill. International Review of Law, Computers & Technology. 16. 317-330. 10.1080/136008602760586769

It is particularly difficult to guarantee the protection of privacy rights in the Indian setting due to the absence of a comprehensive privacy law model. Even though India lacks a thorough legislation on privacy, the problem is nonetheless addressed by proxy. A few proxy laws or event safeguards are being used by the government to protect privacy in the lack of particular regulations. The current Indian legislative framework for privacy leaves the following gaps unaddressed. The absence of a standard for defining data quality, proportionality, and transparency.[2]

Only one framework that addresses the problem of information movement between countries. It's impossible to overlook a legal gap like this in today's technologically advanced world. Using data matching might put your privacy at risk since it requires looking up a lot of people's information without any previous suspicion. When data warehouses are outsourced to other companies like BPOs, this area becomes even more important. Human resources are essential to the effective application of any technology.

People play an important part in the Indian scene since they determine and guide the development of any technology. Social networking sites like orkut, facebook, and others have become popular ways for Indians to stay connected in the age of technology. This phenomenon is known as "community" in India. When it comes to democracy, the media play a vital part by providing information about government policies and the concerns of citizens, yet in today's media-driven society, no one's personal information is protected for their own benefit.

Professor of Cyber Law, University of Leeds School of Law. Indian Journal of Law and Technology publishes the article. Rather than getting hung up on arguments and theories, I'm more interested in the broader cultural implications of these Western-centric problems. Indian privacy rules have long been criticised as being extremely lax.[3]

Because the idea of privacy in India and the West are so different, this assumption is founded on a paradigm that doesn't take this into account. What follows is an argument that one's private life is highly subjective and dependent on one's social and economic circumstances. Due to the hyperbolic reporting by famous Western media outlets on the threat to privacy and data security presented by 'offshore outsourcing,' I became interested in the issue of privacy in India. Only 18% of individuals surveyed in the United States felt the same way about their personal space as the 48 percent of Indians did. Consumer data is not at higher danger in India compared to the United Kingdom or the United States, and there is no evidence that customers in highly regulated nations trust corporations that gather their personal information.

PRIVACY EFFICACY

Today's social patterns and values are too varied, decentralised, and purposely divergent to offer a basis for universal norms of speech at the degree of detail necessary for the protection of private information. While this does not rule out a legal definition of privacy, the legislature may define it as broadly or narrowly it sees proper, taking into account the cultural context and tailoring its contours to meet the needs of the time. It's critical that we dig into these assumptions and reasons in order to better understand the contradictory impacts of India's privacy rules. Freedom, justice, human dignity, individuality, and family life are all intertwined with the notion of privacy. Although the idea of privacy has been around for a long time, it is only recently that this notion has been formalised as a legal right. It is also important to note that when society undergoes a fundamental shift, the idea of privacy must be re-examined. In terms of how far and against what it should be safeguarded, the issue arises. Scholars prefer to define privateness by focusing on a single research project. If privacy is a right to be left alone, it is a basic idea that cannot be applied in a meaningful manner. Clearly, the usefulness of such a skewed interpretation of privacy is severely curtailed. "Not allowing individuals to be alone" is not a violation of privacy, according to Gavison. 6 Therefore, I believe that what constitutes a right to privacy has the potential to have significant ramifications on several levels. As a result, contemporary society's needs and technological advancements necessitate a new understanding of privacy. Is everyone in society guaranteed the same level of privacy protection, and how much privacy is really desired? The right to privacy should be guaranteed to everyone. A person's enjoyment of privacy must thus be subject to the equal entitlement of every other person. However, in practise, this means that everyone will have to give up some privacy. A person's privacy is eroded when others learn about him or her, pay attention to him or her, or get access to him or her, says Gavison. She claims that privacy is a complicated mix of three elements: secrecy, anonymity, and isolation. 7 These aspects are distinct from one another, yet they are linked as well. As a result, privacy is defined as the individual's control over access to, and information about, oneself. 8 A person's right to privacy is unaffected by the fact that others have access to information about him or her that was previously kept private. Any intrusion into someone's private affairs or revelation of someone's personal information would be a

[2] Berisha-Shaqiri, Aferdita & Namani, Mihane. (2015). Information Technology and the Digital Economy. Mediterranean Journal of Social Sciences. 6. 10.5901/mjss.2015.v6n6p78

[3] Minaei, Negin. (2005). IT, TC & Globalization in Emerging New Types of Spaces (Physical & Virtual) in English. 10.13140/2.1.1771.8562

violation of that person's right to privacy if that person decides not to give others access to themselves or their own personal information. As a result, the degree and frequency to which a person is 'exposed' to the public determines the level of their privacy. Some degree of inequity in the distribution of privacy is conceivable as with other social goods.[4]

The primary goal of decisional privacy is to protect people's ability to make important choices free of outside influence. On the other hand, informational privacy addresses the handling, transport, and processing of personal data that is created on a day-to-day basis. (source) What we are renowned for, how accessible we are to others, and how much attention we get from others are all factors in how well-known we are. " 10 This approach has been criticised since the idea of privacy loses its intuitive meaning if a loss of privacy happens anytime any information about a person gets known. As a consequence of this proposal, any loss of an individual's solitary or knowledge about them is now considered a loss of privacy. 11 Wacks12 contends that a limiting or regulating component is necessary, in contrast to Gavison's theory. However, he points out that although concentrating attention on an individual or invading on his solitude is intrinsically disagreeable in and of itself, our concern for the individual's privacy while the person is indulging in activities that we would typically deem private is the greatest. According to him, only information that "relates to the person and which it would be fair to expect him to view as intimate or sensitive and consequently to seek to withhold or at least restrict its acquisition, use, or distribution" should be protected by the law of privacy. 14 "Symbolic of the entire institution of privacy," if the right to privacy were recognised by law, it would only apply to a narrow, customarily delimited, region of information. Thus, it may be argued that access to personal information is a required but not sufficient requirement for it to be characterised as private. In addition, the material must be of a personal and sensitive character, such as information about a person's sexual inclinations, although the substance may also vary greatly from civilization to society.[5]

Stakeholders aren't pleased with the inclusion of data localization rules in the proposed data protection law in India. It is a major part of the Indian government's cloud computing strategy, the RBI's mandate for financial data, and the several data security measures that have been suggested. According to this article, "data protection" rather than "localization" is the way ahead in light of India's previous past and its future economic objectives. There have been two versions of the Personal Data Protection Bill (PDPB) in India since then, the first one in 2018 and the other in 2019. The lower house of parliament approved the measure, and now it is in the hands of the Joint Parliamentary Committee (JPC), which is conducting public consultations.

There are legitimate concerns about the feasibility of segregation and localization in India at the same time. A compelling argument for data localization has been crafted by the Indian government to ensure the safety of Indian citizens' personal information while also ensuring the security of the country. This argument is based on a number of factors, including the need to protect foreign governments' access to Indian citizens' data while also protecting the country's own industry and creating local jobs through the establishment of do Finally, the law is expected to deal with how personal data is secured when crossing international boundaries, reduce "digital trade obstacles," and above all, ensure that Indian individuals' privacy is maintained. Data localization laws exist in several countries, including China and Russia. However, the European Union and the United States have comprehensive and healthy data protection policies.[6]

Today, almost 40% of the global population has access to the internet. In 1995, fewer than 1% of the population had access. From 1999 to 2013, the number of people using the internet more than doubled. Even though the first billion were online in 2005, the second billion in 2010, and the third billion in 2014, a significant portion of the global population, particularly in developing countries in the third world, still do not have access to even the most basic of internet services, creating a digital divide. As a result of the digital gap, there are now those who have and others who do not. Others who have access to the internet and digital sources are seen as superior to those who do not have such resources at their disposal. Digital gap is prevalent in India, one of the nations where it is most apparent. Despite being the third-largest internet user country in the world, behind the United States and China, India continues to be plagued by the Digital Divide. Only 243,198,922 people out of a total population of 1 billion have access to the internet, or 19.19 percent and 8.33 percent, respectively. Inadequate financing, a lack of basic computer and Internet skills, and a lack of English language fluency all contribute to the so-called "Digital Divide," which limits access to and use of digital information resources. Technology has the power to drastically alter the world around us. It's an ever-evolving field that's

[4] Minaei, Negin. (2005). IT, TC & Globalization in Emerging New Types of Spaces (Physical & Virtual) in English. 10.13140/2.1.1771.8562

[5] Long, William & Quek, Marc. (2002). Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise. Journal of European Public Policy. 9. 325-344. 10.1080/13501760210138778

[6] Phahlamohlaka, Jackie. (2008). Globalisation and national security issues for the state: Implications for national ICT policies. International Federation for Information Processing Digital Library; Social Dimensions Of Information And Communication Technology Policy;. 10.1007/978-0-387-84822-8_7

always generating fresh perspectives and innovations. Economic requirement has been universally acknowledged for a workforce that is proficient in the use of information and communication technologies (ICT). With the rise of online communication, such as checking train schedules, buying for groceries, submitting tax returns, and registering your automobile, technology has become a major influence in society as a whole. It has invaded every aspect of our everyday routine. Because of the growing importance of information-intensive industries in today's economy, it is becoming more vital to consider how knowledge is distributed throughout the general population. The widespread availability of the Internet has sparked a debate over its possible impact on society as a whole. Advocacy groups have extolled its advantages, claiming that the technology could reduce inequality by allowing people from all walks of life the opportunity to improve their human capital, expand their social networks as well as search for and find jobs, as well as have greater access to health information. On the other hand, there are many who warn that as the Internet spreads more widely, it will increase inequities and benefit those who are already well-off while limiting development possibilities to those who are less fortunate. In the new IT environment, there are four major digital divisions forming. Each of these four digital divides is intertwined.[7]

To begin with, there is an internal conflict between those who have access to digital technology vs those without it. Both the North and the South have this disparity, but the baselines are different. Language- and culture-based disparities are also present, with the largest dividing line being drawn between the Anglo-Saxon world and other parts of the globe. Inequalities in information technology access between wealthy and less wealthy countries are exacerbating the third divide. Also emerging inside national boundaries is the "digerati," an affluent, information-based elite that is characterised by obsessive focus on cutting-edge technology among young people, disregard for convention and authority, and indifference to the values of traditional hierarchies. There are a number of factors that influence the availability of information and communication technology (ICT). An urban or rural area as well as wealth, education, and age are the most important factors. Income and education are strongly linked to higher access. It has also been shown to be favourably linked to city living (p. 177). Internet connectivity is still mostly an urban phenomena, and it requires a significant overhaul in emerging nations like India where more than half of its population still lives in rural areas where poverty and illiteracy are the norm. There is a concern that the internet is enlarging existing social disparities in India.

Data nationalism has reached a tipping point in cyberspace with India's ban on 59 applications. Cross-border data flows and digital commerce might be affected by the new 'data localisation' requirements that require all app providers to show that their data is not transferred out of the nation. Although data nationalism is just a short-term political movement, it is a manifestation of a deep dissatisfaction with the expanding globalisation over the previous several decades. EC-EIPE researchers found that China, Russia, and Turkey were the most restrictive countries in terms of data localization, with India following closely behind the United Kingdom and other European nations. According to the announcement, the government seeks to safeguard national sovereignty and security by requiring data localization.[8]

This is particularly true in nations like India, where there is a big pool of prospective customers. There are both benefits and cons to data localization. In order to go ahead, both internet service providers and governments must be open and up-front with their customers and citizens about their data collection and use practises.

Privacy is becoming more important as a result of globalisation. Global firms have had to learn about and adapt to different cultures and legal systems all around the globe. "The right to privacy is firmly established in international law," says UNESCO (2012). As a starting point, "Fair Digital Practices" (FIP) provides a good framework for articulating the concepts of privacy in the information age," according to the authors. Personal data privacy has been the subject of law and litigation in both the United States and the European Union during the last four decades. Individuals, business enterprises, government agencies, law enforcement agencies, and national security services have all had interests in shaping how personal data is protected under the law (Cobb, 2016). Lawmakers worldwide have taken note and are working to reduce privacy invasions as a result. Though privacy rights appear self-evident at first glance, national standards for protecting them vary widely. In the EU, for example, privacy rules are far stronger than in the US (henceforth, EU), which indicates that US firms that wish to do business in the EU must meet the EU standard," said Bhasin (2012a). It was recently pointed out by Stevens (2016) that "the EU Data Protection Directive has produced a legislative environment in which each EU Member State has established local data protection rules that reflect their interpretation of the Directive, their local cultural and economic sensitivity." German data protection rules are among the most stringent in the world, whereas Spain's data protection statute requires that passwords be complicated. This has led to nations

[7] Ray, Paula. (2016). Paradigms of Digital Activism: India and Its Mobile Internet Users. 10.1007/978-981-10-0454-4_12

[8] Sarangi, Unmana. (2018). Information Economy and Data Protection Laws: A Global Perspective. International Journal of Business and Management Research. 6. 15-35. 10.37391/IJBMR.060203

like the UK and Ireland being viewed as having a more casual, hands-off attitude to enforcement whereas others like France and Germany are fast to implement strong fines for data protection infringements." As if that wasn't complicated enough, we have to deal with international data protection rules and how EU Member States engage with other nations, particularly the United States. According to the Directive of the European Parliament and the Council of 24 October 1995 on the protection of persons with respect to the processing of personal data and the free movement of such data (see http://ec.europa.eu/), the Article 29: Data Protection Working Group was established. To ensure that personal data can be transferred outside of the EU, the European Commission's (EC) Article 29: Data Protection Working Party (DPWP) has issued 'adequacy' decisions to ensure that the destination country has adequate data protection laws and enforcement; or (b)'model clauses' to which all parties subscribe to bring processing under the EU law (something which is much harder to achieve and manage than might be first thought.[9]

Consequently, firms may now utilise the "US-EU Privacy Shield," a legal framework that can be adhered to by organisations, to accomplish the same results in the event of US transfers. EC and US Department of Commerce recently announced the EU-U.S. Privacy Shield as a successor for the Safe Harbor Framework, as detailed by Sotto and Hydak (2016). There are three main aspects to the agreement: Strong Obligations for Companies' Handling of EU Citizens' Data, Clear Safeguards and Transparency Obligations for U.S. Government Agency Access, and New Redress and Complaint Resolution Mechanisms for EU Citizens." Withdrawal from the EU and the US will have a significant effect on the operations of thousands of businesses of all kinds in both countries, as well as their capacity to undertake cross-Atlantic trade. It is our hope that the 'EU-US Privacy Shield' agreement provides a foundation for firms to reliably transmit data over the Atlantic while preserving individuals' basic rights to privacy and data protection. We applaud the deal. The EU-US Privacy Shield data transfer certification procedure formally started two weeks ago, and applications by US corporations have been delayed," Ashford (2016) recently revealed. There are now just 40 US companies that have been approved under the Privacy Shield transatlantic data transmission scheme. Few businesses have rushed to register for Privacy Shield certification because they are unsure of how the framework will alter and are concerned that it would be challenged. It's also because many US corporations waited until Privacy Shield was enacted and authorised before commencing work on altering their data handling methods to conform with the new framework before submitting their certification applications." A personal identifying code for each individual in a 'ID Card' system is recognised under privacy legislation in Nordic nations, which are not all EU members. Europe's different nations draught and implement their own legislation based on the Directive, which stick to the principles but may vary in detail," according to Bhasin (2008). For example, German legislation does not allow any unsolicited direct mail messages, which are authorised in the United Kingdom, but customers may request not to receive them." According to Privacy International, similar regulations exist in a number of other nations (visit www.privacyinternational.org). Shockingly, the problem isn't as straightforward as first thought.[10]

The right to privacy is enshrined in various ways in the constitutions of the United States, Canada, Germany, and other nations, as well as in legislation. A few examples of nations that have passed legislation to safeguard data and privacy rights are listed by Shah and Zacharias (2010): the United Kingdom; Spain; Switzerland; Sweden; Australia; China (Taiwan); Thailand; Singapore. Furthermore, legislation was established in Sweden restricting the usage of cookies by websites (Bayardo and Srikant, 2003). It's worth noting that the Federal Trade Commission (FTC) has already forced Google and Facebook to sign privacy agreements lasting 20 years, and it's currently looking into additional privacy allegations. Legislation to adopt comprehensive privacy laws for the United States is also floating in Congress. To have a significant impact on the way firms gather and utilise personal data, the federal government has the authority to establish a privacy legislation. There are government privacy commissioners established in most Western nations "to safeguard consumers and educate the public about privacy concerns in general," said Robert (2011). In an effort to address customer privacy concerns, several big Internet corporations (particularly advertising) are deploying their own protections. Among the many firms represented by the Digital Advertising Alliance (DAA) is a system that allows internet users to see which organisations are tracking their online browsing and even advise them to cease displaying targeted adverts, for example. They envision a system similar to the "Better Business Bureau" in which good business practises are rewarded and poor ones are punished.

Data Protection Act No. 152 necessitates the engagement of attorneys and IT experts in the development of systems and procedures for dealing with personal data. Many regulations control privacy and data security in the United Arab Emirates, notwithstanding the absence of an overall federal data protection

[9] Sarangi, Unmana. (2018). Information Economy and Data Protection Laws: A Global Perspective. International Journal of Business and Management Research. 6. 15-35. 10.37391/IJBMR.060203

[10] Berisha-Shaqiri, Aferdita & Namani, Mihane. (2015). Information Technology and the Digital Economy. Mediterranean Journal of Social Sciences. 6. 10.5901/mjss.2015.v6n6p78

legislation. In the United Arab Emirates capital, Abu Dhabi Global Market (ADGM) has been developed as a free zone and an international financial centre. In December 2017, the ADGM also set up an Office of Data Protection (ODP), which was responsible with enforcing and monitoring the rules set out. One of the most important requirements is that the individual in question provide their approval. For electronic payments and stored values, the Central Bank of. has issued a. Users and transaction data must be stored and retained only within the boundaries of the United Arab Emirates (UAE). Even in the telecom business, there are Cernatin limits. In order to guarantee that regulated data is adequately protected, best practises and data compliance measures must be applied. In contrast to other nations, Vietnam does not have a single unified data protection legislation.[11]

As a result, data protection rules are dispersed among a number of laws and regulations. The following laws and publications outline the fundamental principles governing the collection, storage, use, processing, disclosure, and transfer of personal information. Vietnam's many industries and sectors may each have their own set of rules and regulations. There are several factors that determine whether a legal document is applicable to a certain business situation. Some cybersecurity assurance measures are being organised and procedures for their implementation are being prepared for a draught decree. Other legislation presently being created include a Cybersecurity Law and a list of critical national security information systems. Before collecting, exchanging, revealing, or sending personal data to a third party, the data subject must provide their permission. It is essential that regulated data be kept safely and in accordance with international standards that are consistent with ISO/IEC and legislation on the guarantee of cyber-information security. Shari'a principles, which are Islamic principles drawn from the Quran and the Sunnah, are the major basis of law in the Kingdom of Saudi Arabia. Depending on the severity, noncompliance with data protection regulations may result in consequences (including criminal charges). Using worldwide best practises, the KSA Cloud Computing Regulatory Framework (CCF) sets forth the rights and responsibilities of cloud service providers, individual clients, government agencies, as well as private sector enterprises. Allows internal processing choices to be customised to regional expectations by facilitating data residency. Today, our service can be found in over 80 countries and is expanding quickly. Service providers like InCountry assist guarantee that information can be gathered and processed in a manner that fulfils the needs of diverse stakeholders.[12]

Privacy Regulative Scenario in Select Countries: An Overview

With InCountry, business can safely handle your regulated data in over 90 countries, making it possible to grow abroad. Regulated data, such as personal information, must be kept inside a certain nation or area. As seen in the map below, most countries' data-localization regulations are represented. General Data Protection Regulation (GDPR) is an uniform EU data protection regulation that governs the handling of EU citizens' personal data. If a company has to transmit data outside of the EU, they must only do so to countries or organisations who have signed up for similar privacy protections under the GDPR.

The GDPR Implementation Guide for the United States

Restrictive Types of Data

Profile, work, money, health, and payment.

As a result of the Data Protection Act, No. 152 FZ (DPA), which was signed into law on July 27, 2006, Russia has a comprehensive data-protection framework. In the event that Russian citizens' personal data was previously stored in a Russian database and updated as appropriate, Russian data residency legislation does not restrict subsequent processing of this data outside Russia. All Russian firms, branches and representative offices of international organisations, as well as legal entities formed outside Russia, that do not have an official presence in Russia but engage in economic operations in the Russian market are subject to the data localization legislation. You'll have to move your databases to the Russian Federation if any of the aforementioned conditions apply to your business.[13]

[11] Ray, Paula. (2016). Paradigms of Digital Activism: India and Its Mobile Internet Users. 10.1007/978-981-10-0454-4_12.

[12] Madan, Lal & Bhasin, Madan. (2016). Privacy Protection Legislative Scenario in Select Countries. International Journal of Social Science and Business. 1. 1-18.

[13] Ježová, Daniela. (2020). GDPR -RESULT OF GLOBALIZATION?.

II. CONCLUSION

The issue of privacy is not adequately addressed in India's legal framework. An important part of the Make-in-India effort for IT and business process outsourcing (BPO) is the consideration of Digital India. India has passed a legislation to preserve the privacy of its residents' personal information. Data protection, according to this article, is the best course of action in view of India's past and future economic goals. The Digital Divide continues to be a problem in India. As a result, the "Digital Divide" is caused by a lack of fundamental computer and Internet literacy. The administration wants to protect national sovereignty and security by demanding the localisation of data, as stated in the statement. The European Commission's (EC) Article 29: Data Protection Working Group was formed to guarantee that personal data may be moved outside of the EU.

REFERENCES

[1]. Azmi, Ida. (2002). E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill. International Review of Law, Computers & Technology. 16. 317-330. 10.1080/136008602760586769.
[2]. Berisha-Shaqiri, Aferdita & Namani, Mihane. (2015). Information Technology and the Digital Economy. Mediterranean Journal of Social Sciences. 6. 10.5901/mjss.2015.v6n6p78.
[3]. Degryse, Christophe. (2016). Digitalisation of the Economy and its Impact on Labour Markets. SSRN Electronic Journal. 10.2139/ssrn.2730550.
[4]. Minaei, Negin. (2005). IT, TC & Globalization in Emerging New Types of Spaces (Physical & Virtual) in English. 10.13140/2.1.1771.8562.
[5]. Madan, Lal & Bhasin, Madan. (2016). Privacy Protection Laws in Select Countries: Perspectives and Prospects. International Journal of IT, Engineering and Applied Sciences Research. 5. 7-21.
[6]. Mir, Umar & Kar, Arpan & Gupta, Mahabir & Sharma, R.. (2019). Prioritizing Digital Identity Goals – The Case Study of Aadhaar in India. 10.1007/978-3-030-29374-1_40.
[7]. Long, William & Quek, Marc. (2002). Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise. Journal of European Public Policy. 9. 325-344. 10.1080/13501760210138778.
[8]. Phahlamohlaka, Jackie. (2008). Globalisation and national security issues for the state: Implications for national ICT policies. International Federation for Information Processing Digital Library; Social Dimensions Of Information And Communication Technology Policy;. 10.1007/978-0-387-84822-8_7.
[9]. Ray, Paula. (2016). Paradigms of Digital Activism: India and Its Mobile Internet Users. 10.1007/978-981-10-0454-4_12.
[10]. Sarangi, Unmana. (2018). Information Economy and Data Protection Laws: A Global Perspective. International Journal of Business and Management Research. 6. 15-35. 10.37391/IJBMR.060203.
[11]. Sarangi, Unmana. (2018). Information Economy and Data Protection Laws: A Global Perspective. International Journal of Business and Management Research. 6. 15-35. 10.37391/IJBMR.060203.