Journal of Contemporary Issues in Business and Government Vol. 27, No. 2,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

Legal Policies for Sustainable Security and Privacy in Big Data and Information sharing- *A managerial perspective*

K. Sowjanya Naidu
Department of Computer Science and Engineering, Dr. L. Bullayya College of Engg. (W), Visakhapatnam, India

Srinivasa L. Chakravarthy
Department of Computer Science and Engineering, GITAM University, Visakhapatnam, India

ABSTRACT

Information plays an important role as a resource in the development and success of an organization. It is useful in decision-making to achieve the goals of the organization in an optimized way. This has to be achieved without affecting the information security and privacy of the stakeholders. Organizational policies are addressing the above-stated requirements within the jurisdiction and domain of an organization. While accessing and sharing the information among the organizations, the interests of all the stakeholders across the organizations have to be considered. For this, the policies have to be implemented to safeguard the information of the individuals as well as the organization through regulations or laws.

Rapid strides in technology, availability of cheaper computing and networked application environments, high-speed networks, and the increase of data handiness made data sharing very easy across and within the organizations. Data sharing also involves application processing of transactions and analytics in a cloud environment. Sharing in a cloud environment increases the utility but also raises security and privacy issues. Technological changes and domain/legal issues go hand in hand, affecting each other and necessitate changes in laws and regulations. To make the processing of information using big-data and computing infrastructure to be more reliable and secure according to [1] have to be addressed in the design process by considering both technical and legal aspects.

Big data processing is not thoroughly vetted for security issues and is posing challenges to the research community. Laws and regulations have not been crystallized. Existing laws related to common issues are being adopted on an ad-hoc basis.With the growing number of breaches unfolding around the nation and the hacking of government websites, the need to create a safe system for all government agencies has never been more critical. This, at best, is a sub-optimal solution as the current laws and regulations may not be appropriate. This article discusses the prevailing issues related to big-data and the laws to protect them. In addition to that, an attempt

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

is made to analyze several Country's privacy and security laws and regulation which addresses big data security challenges.

Keywords:Big Data Security Challenges, Security & Privacy, Legal Policies, Law Policies,

INTRODUCTION

In recent years, apart from the existing resources like capital, material, human, and machinery resources for the development of an enterprise organization, information also plays an important role. Information can be considered as an input for the product or services. Information is useful as a tool for decision making for the growth of an organization, is also used as a product, and also is taking a part in developments in the smart market growing. In the report [2], the authors present market growth predictions until 2023 on the smart manufacturing industry depicted in Figure 1. In the way of transformation from traditional to digital, termed as digital transformation, many smart emerging technologies such as Augmented & Virtual Reality, Connected Machine Vision, Collaborative Robotics, Self-Driving Vehicles, Drones/UAVs, Additive Manufacturing. The technology growth in the above specific areas impacts the development of industry and hence, the economic growth.

Apart from these advancements of various smart technologies mentioned above, there is another dimension in the advancements, called security and privacy. All these smart technologies and artificial agents communicate with each other and hence, sharing of information takes place between intelligent systems as well as with the environment. Communication between the agents located at severalplaces knockson the door of Bigdata, as it deals with cloud architectures and data sources. The information sharing between all these stakeholders who are the members of the system such as machines, humans, etc., causes a big threat of privacy and security which leads to communication security.

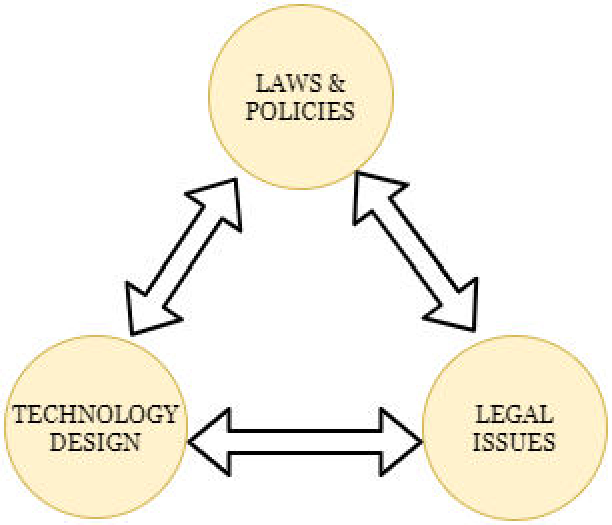

Fig1 : 3 fold design process for Legal laws and Policies

DOI: 10.47750/cibg.2021.27.02.166

Figure 1, shows the three fold design process for legal laws and policies.The technology may raise the legal issues which may provide a path to design of new laws and policies to control the technology consequences. Hence in the design process of computing infrastructure, the design team should integrate the technical aspect to meet the ideas of laws and polices makers or modifications may be included. At the expense of the security and privacy of the customers, the organizations are tending to capitalize. So, there is a need for policies regulations and laws to protect privacy and security in multi stake holder scenario. Private information, especially on the black market, is extremely valuable. The economic motivation to steal private information from malicious people is immense . The government departments and medical facilities have themost detailed information on people and this makes them leading targets for cyber criminals who are trying to profit from stealing this information.

Computer security deals with three fundamental areas namely confidentiality, integrity, and availability. Confidentiality is ensuring that the information is not accessed by unauthorized people. Integrity is assuring the information is not subjected to unauthorized alteration. Availability is the ability to access information in a reasonable time. Any effect on these areas will be affecting the quality of the information, decision making, and thus the overall business. The quantum of impact may be minor or it could be fatal. Because of this, information security is very crucial for the business. So, the organizations are attaching a lot of importance and investing in monitoring and ensuring information security.

The need for Big Data

Nowadays the responsibility of information gained from the available data is traversed beyond the other resources in the path of success of an organization. There is a need of sharing the data across the organizations for their development. In this aspect, organizations may utilize the data in four aspects:

1. Sharing between the organizations
2. From their own generated data
3. Purchase from other organizations
4. Accessing other sources.

All data is disparate and may fall into the categories of structured, semi-structured, and unstructured data. The data (e.g. user data, sensor data, and machine data), which is a great collection encapsulated with intelligence and insights and upon successive examination is termed as Big data [3], [4]. Upon appropriate analysis, big data provides business insight, opensthe latest markets, as well as gives rise to competitive advantages. Several aspects such as Emerging knowledge and social economies, limited information vs information abundance, business stability vs business flux, well-defined industry and industry transformation, global information flow and the emergence of social computing, global digital communities, real-time knowledge flows are the main mainsprings of the Big-Data.

Commodity hardware, technology innovations, growth of open source software, pervasive social networking, and persistent mobile devices combined determines big data. For the growth of the

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

business, variation between real-time data gathering and analysis mission is critical with the advent of big data. The architectures, tools, infrastructure which support real-time analysis are different hence, gaining knowledge from this information should also be distinct. Information sources and content are escalated due to big data, also the pervasiveness of innovation is growing day by day. Due to the variety of sensors from which we expect progressing streams, and are more and more devices are engaged by a system makes data grow rapidly. With storage costs getting low, the cost associated with sparing and utilizing information turns into a non-complicated task [5], [6]. The data centers, servers, storage applications provide enormous log files and isolated data streams that able to be gathered, compiled, and analyzed.

Various security challenges in Big data architecture

Due to digital transformations, for industrial growth, the communication between intelligent agents (either machines or human beings) increased rapidly, hence, massive amounts of data are generated and collected by organizations and companies. They are using that huge collected big data for improving their markets. The data is getting doubled every year which in turn is more beneficial in the development of organizations.

Apart from the advantages of Big data for economic and market growth, the other side of the coin causes the magnification of security and privacy issues. In [7], the authors presented 17 V's and 1 C of Big-Data's characteristics, Volume, Vagueness, Variety, Velocity, Volatility, Veracity, Validity, Value, Verbosity, Variability, Venue, Vocabulary, Visualization, Virility, Versatility, Viscosity, Voluntariness and Complexity made security researchers concentrate more on the security and privacy aspects. The usage of cloud infrastructure on large scale with diversified software platforms that spread across large networks increases the scope of attacks on the system [1].

The present security mechanisms are limited to secure small-scale and static data. It is also difficult to add the security mechanisms to existing cloud infrastructure to reach the ultra-fast demands of security as it is the streaming source of data. In the report [1], the top ten security and privacy challenges and their classification is provided.

- Infrastructure Security.
    - Secure Distributed Processing of Data.
    - Security Best Actions for Non-Relational Data-Bases.
- Data Privacy
    - Data Analysis through Data Mining Preserving Data Privacy
    - Cryptographic Solutions for Data Security
    - Granular Access Control
- Data Management and Integrity
    - Secure Data Storage and Transaction Logs.
    - Granular Audits
    - Data Provenance

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

- Reactive Security
  - End-to-End Filtering & Validation.
  - Supervising the Security Level in Real-Time.

Legal challenges & Regulations

Big data processing is not thoroughly vetted for security issues and is posing challenges to the research community. Laws and regulations have not been crystallized. Existing laws related to common issues are being adopted on an ad-hoc basis. This, at best, is a sub-optimal solution as the current laws and regulations may not be appropriate because of:

- Non-scalability of encryption for huge data sets
- Non-scalability techniques in real-time monitoring systems for smaller data
- Heterogeneity of devices that produce the data
- The abundance of diverse legal and regulatory policies leads to confusion

Organizations are tending to capitalize on this limitation at the expense of the security and privacy of the customers. Thus there is a need for designing laws and regulations apt for big data security. This article discusses the prevailing issues related to big-data and the laws to protect them. Considering the top ten big-data security and privacy issues recognized by Cloud Security Alliance (CSA) [1], an attempt is made to provide regulations and laws of various countries.

The technology may raise legal issues which may provide a path to the design of new laws and policies to control the technology consequences. So, in the design process of computing infrastructure, the design team should integrate the technical aspect to meet the ideas of laws and policymakers or modification s may be included. Figure 2, shows the three-fold design process for legal laws and policies. At the expense of the security and privacy of the customers, the organizations are tending to capitalize. So, there is a need for policies regulations, and laws to protect privacy and security in the multi-stakeholder scenario.

Global Applicability of the Policies: Policies are generally applicable within an organization. Laws are specific to a political nation and limited to boundaries of the nation whereas regulations are made and monitored by some of the influential non-political organizations and international regulatory bodies which are honored by all stakeholders. In certain ways, various countries may group to follow the regulations.

RELATED WORK

Three Phases of Big-Data

According to [8], however, the word Big Data has been using for three decades but it is not perfectly new and the essence has been using for data analysis to support their decision-making process. The three main phases of Big-data which mainly used for data analysis are provided as:

- Phase I (1970-2000): DBMS-based structure content and Data Warehousing were major core components. Querying, optimization, extraction, are key techniques used for

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

analytical processing. In addition to this phase was adopted data mining and statistical analysis

- Phase II (2000-2010): Apart from the structured data, due to tremendous changes in internet and web development, there was an increase in semi-structured and unstructured data. In addition to the traditional structured data types, companies had to find innovative methods and storage strategies to deal with these new data types to analyze them effectively. The arrival and development of social media data have significantly exacerbated the need for tools, software, and analytical techniques to obtain useful information from this unstructured data.
- Phase III (2010- to date): Data transferred as wealth. Organizations having more focus on collecting data by adopting the advantage of emerging mobile services and usage. In addition to that growth in AI and IoT technologies, industry 4.0 is formed. New approaches like HCI, Mobile visualization, location-aware analysis, self-driving cars, etc are using concepts of Big-data.

Technology Evolution of Big-Data

- Batch processing (2003-2008): Huge collections of data are gathered, processed, and then results are produced for a batch. To handle fault-tolerance and scalability issues, DFS is used. To improve efficiency, Parallel programming models are used. Examples: HDFS, Apache Hadoop, MR, GFS.
- Ad-Hoc Processing(2005-2010): To overcome shortcomings of DFS which are appropriate for sequential data access, random read/write access is used. This issue is solved by NoSQL databases by considering column-based or key-value stores. In addition to that, it supports for storage of large unstructured datasets like graphs and documents. Examples: MongoDB, CouchDB, HBase,
- SQL (2008-2010): The data stores are accessed through very simple interfaces to query. The mechanisms of this approach and functionalities are as same as the traditional data warehousing mechanisms. Examples: Google Planner, HStore, Apache Hive/Pig, PrestoDB.
- Stream Processing(2010-2013): Before storing them data is continuously pushed to servers as streams for processing. Streaming data contains incoming patterns thatare unpredictable. Such data streams are processed with solutions that are fast, fault-tolerant, and highly available. Examples: Apache Kafka/Storm, Hadoop Streaming, Apache Drill, Google Big Query, Samza Apache Flume/Hbase, Google Dremel.
- Real-Time Analytical Processing(2010-2015): The live channels and machine-to-machine applications generated data streams which makes us take decisions automatically. These architectures help to apply real-times rules for the incoming events and existing events within a domain. Examples: Google Data flow, Amazon Kinesis, Apache Spark.
- Intelligent Systems (2014-to date): The data is rapidly generating wherever and whenever the GPS-equipped smart devices like mobile phones and intelligent machines like UAV

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

are connected through high-speed internet. The communication between intelligent agents in the era of digital transformation generates streams of data.

Recent Impacts of Big Data on Industry 4.0

Two study technologies, Artificial Intelligence and Machine Learning transformun-widely big-data into an approachable stack. Several practical domains like dynamicpricing, video analytics, customer churn modeling, etc., in which the above saidtechnologies are employed to enable the business in algorithmic approach. The organizations which are spending revenue on AI & ML are expecting 39% of growth.According to [9], IDC estimates the spending revenue on AI & ML will hike by $ 57.6 billion in 2023.

As a prediction, next decade Quantum computing will take big data into its hands of data analytics and hence it will be a big stack holder in the future generation. Collecting the data at which it is being captured without storing it in central data locations, termed as Edge analytics, used for data analysis will also make an important role in big data and inturn in the Industrial growth. Ever-growing sensor information like video, text, voice changes almost all business models. Organizations wanted to do business according to customer's views and interests, hence trying to adopt big data and cloud architecture to run their operations most efficiently. According to IBM, by 2020, the Dark Data category captures about 93% of all data. Thus, big data in 2020 will be included in Dark Data.

Challenges:

Big Data provides a platform of opportunities in the development of the economic wealth of an organization, however, it is also carving new provinces and problems that are seeking special attention and upon failure, it can raise business threats not only in terms of reputation but also financially and legally. According to the literature review, the organizations who wants to make wealth with the help of Big Data must be addressing the concerns of:

- Data privacy: People may lose their rights to keep their data private, as big data generates data that contains a lot of information about our personal lives.
- Data security: Even if we decide to provide our information to someone for a purpose, we are unable to trust them whether they keep it safe.
- Data discrimination: We will try to discriminate against people based on data available about their lives, even though everything is known, may not be acceptable. For example, credit scoring is used to decide to provide lending money and insurance and it is heavily data-driven.
- Data quality: More raw data is being collected according to the trend with technology and it is very closer to the end-user. The prime hazard is the data in raw format is sensitive towards quality. The jeopardy increases when we try to reduce the gap between the end-user and raw data. Not more concern has been given on quality and contextual relevance.

The Economist Intelligence Unit, in their report 2015, mentioned the importance of security and privacy. Even top-notch organizations are also facing struggles with several technical facets of big data. These underpinned facets of data management still go deep in to facilitate more up-

DOI: 10.47750/cibg.2021.27.02.166

coming, the value-added facet of data management. The data management may be governance, compliance, and converting data into considerable perceptions. 29 % organizations financial performance ahead of peers ensuring security and Privacy and 25% organizations financial performance at par with peers ensuring security and privacy. 21% of an organization's financial performance are ahead of peers ensuring good data governance like integrity, security, usability, availability, and 19% of organizations' financial performance at par with peers ensuring good data governance like integrity, security, usability, and availability. 32% of organizations utilize cloud technologies for information security big data efforts. 28% Security challenges by an organization and 20% for good governance[10].

ASPECTS OF LAW IN BIG DATA

Problems in security pose a serious threat to the system, which is why it is crucial to process the gaps in the security. Big data is nothing naive to large organizations, however, it is gaining popularity among the small and medium firms as well due to the reduced cost of storing and easy management of data. Cloud-based storage also facilitates huge data storage. The maximum of the security issues are caused by the lack of effective measures provided by the firewalls and anti-virus software's of the systems which are developed to protect the information stored in the disk, but big data is much more when compared to that.

Hence, due to the increased storage of data, the data is posed with serious security and privacy threats. The concern with the highest priority to companies using Big data is providing security to cloud-based systems. If the cloud-based systems are targeted, the transfer of the data by malware can be done without raising any suspicion [11]. The legal issues in the big data scenario are not about just how to gather the data, but how you use it. Hence the data used in malicious ways may lead to legal issues for both the individual as well as firms. However, big data has serious limitations and dangers when applied in the legal context. These limitations can lead to generating unintended consequences in the legal system.

The breaches in Big data are putting forward a challenging task for law enforcement. The need for the setting up of the boundaries is an immediate task in emerging data markets. Some of the key areas on the list are:

- Digital Legal Pluralism means having multiple legal systems in any particular geographical area. The jurisdiction remains the same but has differentlegal systems.
- Balancing the citizens' rights and security digitally. Here the citizens' rights are meant to be the rights regarding the data and security is meant to how to deal with the rights of the individuals and the needs of the individuals.
- The need of the hour is the global digital legal culture. Digital legal culture meant the temporary outcomes of interactions to the challenges and response paradigm. The need to analyze the legal paradigms shapes the distinctive legal culture. Global digital legal culture meant the mix of digital laws all over the world.
- The National and International legal frameworks have to be enhanced which fits the new digital concepts and terminologies and allowing legal interoperability across different jurisdictions and cultures worldwide. Many of the countries are unaware of the digital

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

trends and breaches taking place and are only following the old traditional laws which are being operated with the vulnerabilities. Hence the legal frameworks of national and international grounds have to be available in equal to all the data breaches taking place.

- Building social consciousness where privacy should be acknowledged as a social and collective responsibility of preserving the data.
- The legal and technological issues are some of the umbrella activities were identifying the knowledge about safety and security of the data and the metadata.
- The key point is the development of the measures to be taken from the technical point of view where the design of privacy and data protection should be developed. Encryption, Decryption, and other protocols should be developed with ethical and legal protection.
- Ethics also play an important role in the institutional system.

On par with the technological advancements and developments, Big data analytics have thoroughly changed the way how law enforcement and security agencies are examining information. Hence the legislation governing the functions should be focused on 20th-century trends instead of using the then existing laws for safeguarding personal data. The governments and law enforcement agencies are moving towards the modifications of laws to play a pivotal role in regulating the use and misuse of the data.

Big data is playing a minor role in many developing countries as of now but it is set to become increasingly popular in the coming years. It is estimated that Big data will play a major role in the coming years from now and will have a greater impact on government, public, private, and people's lives. Onthe other side of the coin, apart from the benefits which can be reaped from big data, there is also a downside when the data of the firms or individuals is at stake. Hence the governments are investing millions of rupees in big data Projects which are beneficial for using as well as safeguarding the data. Some of them are:

- The US reserved $ 200 Million for development and research on big data which can be used in all the spheres of government organizations.
- The UK spent 159 million on high-quality and network infrastructure, and 189 million to develop the UK's data infrastructure and support big data applications.
- In South Africa, the government invested 2 billion South African Rand in the Square Kilometer Array project which wheels around complex data sets.
- In France, research projects related to Big data were awarded 11.5 million.
- In Germany, the Ministry of Education and research invested 10 million in Big data research institutes.
- India launched “Digital India ” programme to transform india into a digitally empower society and knowledge economy to present huge potential to Big data analytics.

The governments are eager to start Big data projects by investing huge amounts of rupees. The governments apart from investing also should concentrate on formulating future-proof legal policies, as to how beneficial Big data is to the governments.There is always a risk from the

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

whistleblowers who bring the confidential files out of their reasons. As Big data is taking a positive sphere, the negative sphere also arises. The confidential data kept by the big data mechanisms can be leaked by the whistleblowers who either for the public or personal interest expose the sensitive information or activity within the organization that is deemed illegal or unethical. There are also laws designed to protect the whistleblowers who for the benefit of society bring allegations to light in organizations, governments, or any agencies [12].

Need for Laws and Regulations

To the best of our knowledge, according to the literature survey, in most of the countries, the rules existing in the area of privacy and security in data protection are being applied to the Big Data processes. The Data Protection Agencies (DPA) in several countries play an important role in the protection and preserving of data of the individuals. Several Data Protection Agencies strongly recommend that the prevailing data protection principles must be enhanced to meet the requirements of bigdata processing and maintenance.

The UK DPA states that data protection rules apply to big data processes as well. Protecting the data poses a serious threat when the data is collected without consent or gathered from connected devices which are collected unconsciously from the individuals or firms. Big data dispose of the data for unknown and unusual purposes by which the limitation principle might be violated. The data which is used for big data processing might also violate the data minimization principle. The data minimization principle states that the data gathered and processed should not be availed withheld unless it is essential or it can be utilized for reasons which should be mentioned and meaningful [13], [14].

The French DPA proposed a new law called “The Digital Republic" with the help of the people by putting an online consultation to the public where they can suggest amendments ranging from net neutrality to open data. Despite this fact, steps are taking place for new dangers posed by big data and proposing new legislation that specifically addresses these issued. The DPA's opine that the new legislation can give support to face the issues raised of big data.

The question that now arises is that whether it is advisable to formulate new policiesfor Big data processes. The issues which have to address are:

- The current framework and its underlying principle could not be answerable to the new risks which big data poses.
- The current framework which is based on traditional approaches is restrictive to the private firms to adopt new technologies.
- The current framework could not be applied appropriately in the interpretation of big data.

Keeping the above points in consideration, the new regulatory scheme might provide a solution for the issues presented above. Since the data protection law is growing rapidly, a few gaps still exist. Some of the countries have not formulated any laws in the data protection area, and some countries have partial laws, and some laws are outdated as mentioned in the above points. The countries which are still formulating the laws should develop legislation that covers a wider range [15], [16].

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

Laws policies in various countries

Driven by the rising concern about the possible vulnerability of networked societies and the number of cyber-domain disturbances, many countries have taken steps to better understand the vulnerabilities and threats to which their (information) infrastructure is subject, and have proposed measures to secure these assets in the form of guidelines and regulations. Below are some countries to advance towards the field of formulating laws in big data issues.

United Kingdom

UK implemented the Privacy and Electronic Communications Regulation (PECR) for E-privacy which led to the formulation of the General Data Protection Regulation (GDPR) and the act named Data Protection Act 2018 (DPA 2018). The GDPR applies to the processing of the personal data on personal interest, regardless of where the processing takes place under Article 3(1),GDPR [17], [13].

Even though the UK parted from the EU, the GDPR applies to everyone equally. Considering an example, if the controller who processes the purpose and means of data is in the UK or elsewhere in the EU, the GDPR applies the same. The GDPR included profiling which is taken as any form of processing of personal data that is used to estimate certain aspects of any person in the big data processing is dealt with under Article 4(4),GDPR [18].

Article 5(1) (a) of GDPR deals with the role of the controller of the data. The GDPR requires that the acceptance be given freely, unambiguous, informed, and specific of the subject whom he/she would give clear and affirmative action to be processed under Article 4(11), GDPR. Public authorities' legitimate interests are dealt with in Article 6(1)(f). All the other data protection principles are dealt with in Article 5, GDPR. The principle of data minimization is explained in Article 5(1) (c) [19].

United States of America

In the United States, unfortunately, there is no single law for data protection but a jumble of hundreds of laws to protect the personal information of US residents at both federal and state levels. In the USA, the laws are typically sector-specific i.e., the laws focus on a particular type of data. A few examples are quoted below [16], [19], [20].

- The Drivers Privacy Protection Act of 1994 governs the privacy and disclosure of personal information gathered by states Department of Motor Vehicles which includes SSN, Driver Identification Number, Name, Address, etc.
- Children's information is protected at the federal level under the Children's Online Privacy Protection Act which prohibits the collection of the data of any child under 13 years of age if needed so it requires parental consent.
- The Gramm Leach Bliley Act(GCBA) governs the protection of personal information in the hands of banks, insurance companies in the financial service industry.
- The Health Information Portability and Accountability Act (HIPPA) protects the information of the individuals regarding the health status and health care of the individuals.

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

- The Telephone Consumer Protection Act (TCPA) deals with the calls, messages to the individuals and regulates the marketing calls to the people.

Hence, the laws in the US are sector-specific, there will not be a controller as specific and each sector takes care of the rights designed to the people.

Canada

Privacy in Canada is regulated through a mix of the constitutional, statutory and common law. The fundamental protection is provided by Section 8 of the Charter of Rights and Freedoms which explicitly states that Everyone has the right to be secure against unreasonable search". Some laws apply to the collection and disclosure of personal data by different organizations in both public and private sectors at all levels. Organizations in both sectors require laws to defend privacy-related lawsuits and torts. The Parliament of Canada is considering the recommendations to enact rules and guidelines related to data ownership and data sovereignty to put a stop to the non-consented collection, use, and disclosure of citizens' personal information [21], [22], [23], [19].

The Canadian Big data framework exists in different layers. Though there are 7 layers, we deal only with the first 3 layers which deal with the privacy of the data of the individual.

1. *Layer 1*:This layer involves core privacy legislation at federal and constitutional levels. Some of the important laws for the data protection imbibed in layer 1 are discussed below.
    a. The Personal Information Protection and Electronic Documents Act (PIPEDA)" was enacted in 2018. It applies to the personal information of the private sector and employee information of the public sector.
    b. The personal information held by the federal government institutions is covered by Federal Privacy Act.
    c. Canada's "Digital Charter" is the foundation for policies of the federal government for a people-centered data and digital economy.
2. *Layer 2:*This layer applies to and replaces the material parts of PIPEDA with some of the acts mentioned below.
    a. British Columbia's Personal Information Protection Act.
    b. Alberta's Personal Information Protection Act.
    c. Quebec's An Act for Protection of Personal Information in Private Sector.
3. *Layer 3*: This layer applies to the territories which cover both public and private activities and has a huge number of Acts imbibed in them.

India

India is one of the latest entrants in the field of data, protection, and security. The Information Technology Act (2000), amended by the Information Technology Act (2008) contains the provisions for the protection and security of electronic data [24].

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

The Cyber Contraventions under sections 43(a) to (h) and cyber offenses under sections 63 to 74 from the Information Technology Act (2000). Under section 72A of the Information Technology Act, 2000 disclosure of information intentionally without the consent of the person is a breach in the lawful contract and is a punishableoffense with imprisonment for 3 years [25].

Section 65 of the Information Technology Act deals with the tampering of documents either knowingly or unknowingly shall be liable to the imprisonment of up to 3 years. In April 2011, the SPD rules under section 43A of the IT act as Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data of Information Rules,2011).

The draft Legislation called the Privacy Bill was introduced in 2011 which recognized the individual's right to privacy of data. After many iterations, the bill was released over six years. The major leap took place with the Personal Data Protection Bill drafted by the Sri Krishna Committee and approved by the cabinet of the government of India. Several features are discussed and submitted by the Committee some of which are Data Judiciary, Data Processor, Territoriality, Exemption, Grounds for processing personal data, Transparency, Accountability, etc., [26], [27].

The personal data Protection Law is set to govern the collection, storage, and processing of data by private and public entities. Some other acts which deal with Data Protection are:

- The Copyright Act (1957): This Act protects the intellectual rights in different types of works including literary works which include databases, copying the computer database, distributing the database could amount to Copyright Infringement Act.
- The Indian Penal Code (1860): This is used to prevent the theft of the data.
- The Indian Constitution: Article 21 of the constitution protects an individual right to life and personal liberty. The Supreme Court of India in the nine-judge bench decision in Justice Puttuswamy Judgment held that the right to privacy is an intrinsic part of the fundamental right of life and personal liberty under Article 21.
- The 2013 National Cyber Security Strategy was designed to create healthy and resilient cyberspace for the people and businesses of India.The Ministry of Electronics and Information Technology said the policy is aimed at protecting cyberspace information and information infrastructure, building capacity to prevent and react to cyber-attacks, reducing vulnerabilities, and mitigating cyber incident harm through a combination of institutional frameworks, individuals, processes, technology, and cooperation.

The new data privacy authorities intend to safeguard the user's fundamental right to privacy from risks of unwanted exposure of people's sensitive data in this digital era. Data protection laws have impelled organizations to draw up stringent measures for protecting user's data from any kind of threat, data leakage, or cybersecurity breach. The end goal is to secure the digital citizens in all aspects from data breach and hence penal actions are needed in the majority of data protection enactment.

DOI: 10.47750/cibg.2021.27.02.166

CONCLUSION

Big data is useful in decision-making to achieve the goals of the organization in an optimized way. In the way of utilizing Big-Data, the information security and privacy of the stakeholders are at a sharp edge. Organizational policies are addressing the above-stated requirements within the jurisdiction and domain of an organization. For this, the policies have to be implemented as regulations or laws. Sharing in a cloud environment increases the utility but also raises security and privacy issues. The advent of Big data in this era is posing serious security issues.Technological changes and domain/legal issues go hand in hand, affecting each other and necessitate changes in laws and regulations. To make big data processing and computing infrastructure more secure accordingly have to be addressed in the design process by considering both technical and legal aspects.The authors presented laws and policies made in various countries and an acute analysis of each country.

Future direction: Big data processing is not thoroughly vetted for security issues and is posing challenges to the research community. Laws and regulations for safeguarding the data of the firms and individuals have not been crystallized. Existing laws related to common issues are being adopted on an ad-hoc basis. The laws and regulations which are existing now only provide a sub-optimal solution as the laws and regulations which are taken for Big data processing are inappropriate. The authors in this articleattempted to discuss the prevailing issues related to big-data and the laws to protect them. Considering many security and privacy issues, an attempt can be made to design a framework to deal with big data security challenges and comply with regulations and laws for many countries in the future which can be accepted globally.

Funding information if any:

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

Report on Top 10 Big Data Security and Privacy Challenges. (Nov. 2012 (accessed April 2020)). https://www.securitymagazine.com/articles/84461-top-10-big-data-security-and-privacy-challenges-reportreleased

Industry 4.0 & Smart Manufacturing 2018-2023. (Nov. 2018 (accessed April 2020)). https://iot-analytics.com/product/industry-4-0-smart-manufacturing-market-report-2018-2023/

REPORT TO THE PRESIDENT BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE. (May 2014 (accessed April 2020)). https://bigdatawg.nist.gov/pdf

Jain, P., Gyanchandani, M., Khare, N.: Big data privacy: a technological perspective and review. Journal of Big Data 3(1), 25 (2016)

Moura, J., Serr~ao, C.: Security and privacy issues of big data. In: Cloud Security: Concepts, Methodologies, Tools, and Applications, pp. 1598{1630. IGI Global, ??? (2019)

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

Gholami, A., Laure, E.: Big data security and privacy issues in the cloud. International Journal of Network Security & Its Applications (IJNSA), Issue January (2016)

S, A.P., S, V.S., A, V.K.: The 17 v's of big data. International Research Journal of Engineering and Technology 4(9), 5 (2017)

Framework, E.B.D.: A Short History of Big Data. (May. 2019 (accessed April 2020)). https://www.bigdataframework.org/short-history-of-big-data/

FRAMINGHAM: New IDC Spending Guide. (Sept 2019, (accessed April, 2020)). https://www.idc.com/getdoc.jsp?containerId=prUS45481219

Limited, T.E.I.U.: Report on Big Data evolution: Forging New Corporate Capabilities for the Long Term. (2015 (accessed April, 2020)). https://www.manpowergroup.com/wps/wcm/connect.

Devins, C., Felin, T., Kau man, S., Koppl, R.: The law and big data. Cornell JL & Public Policy 27, 357 (2017)

Casanovas, P., De Koker, L., Mendelson, D., Watts, D.: Regulation of big data: Perspectives on strategy, policy, law, and privacy. Health and Technology 7(4), 335{349 (2017)

Kemp, R.: Big Data and Data Protection (GDPR and DPA 2018). ((accessed April, 2020)). https://tinyurl.com/y8ofws5g

Sumy, R., Natalie Donovan, S., May: AI and Data Protection: Balancing Tensions. (July. 2019 (accessed April 2020)). https://tinyurl.com/ydds7tjj

Mike Rebeiro, M.R.S.C. Malcolm Walton, Taylor, S.: Big Data and Competition Law: with Great Opportunities Come Great Risks. (June. 2019 (accessed April 2020)). https://tinyurl.com/y8jwxaut

Chabinsky, S.: USA: Data Protection 2019. (July. 2019 (accessed April 2020)). https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Society, R.: Data management and use: Governance in the 21st-century British academy and royal society project (2017)

Group, R.S.W., et al.: Machine learning: the power and promise of computers that learn by example. Technical report, Technical report (2017)

Van der Sloot, B.: International and comparative legal study on big data (2016)

Myers, C.: Big Data, Privacy, and the Law: How Legal Regulations May A fact PR Research. (Jun 2018 (accessed April 2020)). https://instituteforpr.org/big-data-privacy-and-the-law-how-legal-regulations-may-aspect-pr-research/

Phull, C.: The Framework of Big Data Law in Canada, and Its Privacy Law Core. ((accessed April 2020)). https://www.smartblocklaw.com/blog/big-data-law-in-canada-ch2

Brown, S.: The Privacy, Data Protection, and Cybersecurity Law Review - Edition 6, Canada. (October 2019, (accessed April 2020)). https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-lawreview-edition-6/1210002/canada

P-ISSN: 2204-1990; E-ISSN: 1323-6903

DOI: 10.47750/cibg.2021.27.02.166

Big Data Guidelines. (May 2017, (accessed April, 2020)). https://www.ipc.on.ca/wp-content/uploads/2017/05/bigdata-guidelines.pdf

MeitY: DATA PROTECTION IN INDIA. (FEB 2018, (accessed April, 2020)). https://digitalindia.gov.in/writereaddata/les

Gupta, N.: Data Protection In India. (Oct 2018, (accessed April, 2020)).https://www.mondaq.com/india/privacy-protection/744160/data-protection-in-india

Subramaniam, H.: India:Data Protection 2019. (July 2019 (accessed April 2020)).https://iclg.com/practice-areas/data-protection-laws-and-regulations/india

Subhajit Basu, R.M.: BIG Data: A Challenge to Data Protection? ((accessed April, 2020)).https://www.indialawjournal.org/