International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 05-11-2019; Accepted: 08-12-2019
www.lawjournals.org
Volume 6; Issue 1; January 2020; Page No. 26-30

Recent data protection regulations: For protection or violation of privacy/ A detailed analysis

Tejash Bhandari
Kirit P. Mehta School of Law (NMIMS), Mumbai, Maharashtra, India

Abstract
In the beginning of the paper the author will be discussing how the data protection laws of India evolved in these years and the recent amendments to data protection laws as well as the recent K.S Puttaswamy v Union of India judgement. This paper further serves the purpose of briefing the reader about the recent data protection laws introduced by countries viz. India, California, Russia and Spain and how these stand in violation of data privacy of their citizens. So, the purpose for which these laws were enacted in the first place, were not fulfilled as these laws violated data privacy themselves. Throughout the paper various loopholes are pointed out in these laws while analysing them. At the end, suggestions are given which elaborate laws enacted in other countries and how they have served their purpose of data protection rather than restricting citizen's privacy. All the major countries data privacy laws which led to resentment in recent times are analysed in this paper so that similarity and common loopholes can be drawn between these laws.

Keywords: data protection, privacy, violation, citizens

1. Introduction
The most basic definition of data is information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer. [1] There are 2, considerably related topics which will be discussed in this research paper throughout those are: data protection and data privacy. Data Protection means "laws and regulations that make it illegal to store or share some types of information about people without their knowledge or permission." [2] Data privacy means to keep one's personal matters secret available in e form. In some recent laws made by various countries it is observed that the latter is overlapping the former. As also quoted on the website of European data Protection Supervisor "Privacy and Data Protection, though connected, are commonly recognised all over the world as two separate rights" [3]. Right to privacy in India was recently recognized by the Hon'ble Supreme Court of India in K.S Puttaswamy v union of India [4] under Article 21 of the Indian constitution. The increase in digital data has forced governments to bring in stricter laws for protection of data of individuals of the state. The Governments worldwide have tried to protect data of their individuals but in the process of protecting their data sometimes governments tend to do more which can harm privacy of individuals and corporate business.

2. The current approach: India
The first and only legislation passed related to online data was the Information Technology Act, 2000 which contains provisions relating to cybercrimes and data breaches. The preliminary of the act reads as follows "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto." [5]

In 2008 this act was amended because the act prior to amendment only included government agencies and not individuals or companies as also mentioned above in the preliminary of the IT Act, 2000. The amendment introduced sec. 66A which included sending offensive messages by means of computer resources. There were many cases in which offenders were booked under this section which led to wide criticism of this section. It was seen as violator of Article 19 (1) (a) of the Constitution of India. In 2011 the act was again amended to include Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011 ("SPDI Rules") under sec. 87(2).

This inclusion of SPDI rules was the first step towards data protection of individuals as well as corporate information. This can also be regarded as the first step towards granting Right to Privacy as a fundamental right. In 2015, the Supreme Court of India gave the verdict that Section 66A is

unconstitutional in entirety. The court said that Section 66A of IT Act 2000 is "arbitrarily, excessively and disproportionately invades the right of free speech and upsets the balance between such right and the reasonable restrictions that may be imposed on such right," said a Bench of Justices J. Chelameswar and Rohinton F. Nariman. The definition of offences under the provision was "open-ended and undefined", it said. Provided under Article 19(1) of the Constitution of India. But the Court turned down a plea to strike down sections 69A and 79 of the Act, which deal with the procedure and safeguards for blocking certain websites. [6]

With increased digitisation there was a need felt by the legislators to introduce a more specific act related to personal data privacy. Although the IT act contained all the necessary provisions relating to data protection, but with technological advancements and new techniques of committing cybercrime the act was deemed to be necessary. Keeping in mind the above requirement Justice B.N Srikrishna committee was constituted which was headed by Former judge of Supreme Court of India. According to the government order, the terms of reference of the committee include, "To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill." [7]

In 2017 Supreme Court of India gave an important constitutional judgement regarding Right to Privacy declaring it a fundamental right under article 21 of the Constitution of India. The case started with Justice K.S Puttaswamy (Retired) filing a petition in Supreme Court challenging constitutionality of Aadhaar card on the grounds that it violates right to privacy. The centre argued that Right to Privacy was not a fundamental right. The case was then referred to a Constitution bench. The conclusions are set out at pages 260-265 of the joint judgment. It is held that privacy is a constitutionally protected right which emerges, primarily, from Article 21 of the Constitution. This is not an absolute right but an interference must meet the threefold requirement of (ii) Legality; (ii) the need for a legitimate aim and (iii) proportionality (p.264). It is also noted that, as informational privacy is a facet of the right to privacy the Government will need to put in place a robust regime for data protection. [8] This judgement added more importance to data protection laws as privacy was declared a fundamental right. The judgement also gave another aspect to see data privacy laws as they cannot violate privacy of individuals by the hands of the state was clearly stated in this case.

On 27th July, 2018 the committee submitted a report titled 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians' and a draft of Personal Data Protection Bill, 2018. The bill is combination of rules of EU's GDPR and data protection laws of other countries. The data under this bill will be divided in two parts critical which can include defence or financial data and non-critical which should be deleted in some time. It proposes that how corporates can store the data and how long can it be stored. The data which is important can be stored by government and also a check is introduced to see if the data circulated does not defame the government.

The data which is to be stored by corporates including foreign firms can only be stored locally in the country so whenever of use can be taken by Government. This clause will affect all major technology giants which operate in India from foreign. The bill should be abided by all the corporates as well as individuals which operate with data of Indian citizens. Failing to meet these provisions can cost companies dear, with the bill laying down penalties that can go up to ₹15 crore or 4 per cent of a company's total worldwide turnover. [9] The bill has many shortcomings because in a very short term government has attempted to create a very complex legal framework for data protection.

First problem is the clause of saving data of users in India which will make functioning of foreign firms in India very hard and in turn affect the Indian economy badly. Second and one of the major purpose why this law was introduced will get hamper because the state has access to all user data. The state is not always neutral as the ruling party can use the data to fulfil its own purposes. The best example of this problem is the recent case of Russia where many government sites have leaked data viz. full names, job title and place of work, emails, and tax identification numbers, etc. It can also be used to detain, investigate charges where the government is criticized in the name sedition.

Although the data protection bill is not a bad effort given how little time drafters had to produce it, the legislation is far from ready for enactment. The government might do well to consider its own internal drafts, some of which did a superior job of avoiding the various privacy risks that the new data protection bill creates. [10]

If the above act was not enough to harm data privacy of citizens a new order was released by the government of India in December which stated that 10 government agencies can intercept or examine any computer for any information which it seeks. The gazette was issued under sec.69 (1) of IT Act, 2000. The government's explanation for this move was that only order was issued under section which was in existence at the time when this act was passed. People who don't follow this order will be held guilty under IT act and may face 7 years imprisonment and fine. This order will have the same effect which will be caused by passing of the personal data protection bill as this will also harm the privacy of citizens and can be misused by agencies as well as by the government.

A similar controversial Australia's Assistance and Access Bill 2018 was passed by Australian parliament in December. The bill is set to be applicable by 2020 and is estimated to be followed by then. The law is introduced as an anti-encryption bill and gives government power to force tech companies to give data of any citizen of Australia and to make it mandatory for companies to cooperate with government, penalties will be imposed on non-complying companies. The only difference between the Indian notification and this bill is the notification only talks about snooping on computers but in this bill all encrypted data with tech companies will also be exposed. This will lead to

more no. of hackings as all encrypted data will be decrypted by government for use.

3.1 Worldwide data protection

3.1 United States

In 2018 lawmakers of California passed California Consumer Privacy Act which aims to provide stringent data protection laws to protect data of citizens of California from big tech companies. The law predominantly focuses on restricting use of consumer data by large businesses, defined as having annual gross revenues in excess of $25 million, or having received personal information for 50,000 consumers. In short, Facebook would be affected, but probably not most start-ups, depending on the details of their business. [11] After introduction of the act various bills were introduced to amend CCPA. These bills were widely criticized as changes these will bring to CCPA will lead to serious data privacy violations some of which are deliberated below.

Assembly bill 25 reads as under

"This bill would exempt, from all provisions of the act, except the private civil action provision and the obligation to inform the consumer as to the categories of personal information to be collected as described above, information collected from a natural person by a business in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business, as specified."

The bill implies that any person employed at any position in a company is exempted from protection under CCPA. So, the business can collect and use employee data for any purpose.

Assembly bill 846 reads as under

"The bill would prohibit a business from selling the personal information of consumers collected as part of a loyalty, rewards, premium features, discounts, or club card program. program, subject to specified exceptions, including that the business is authorized to sell the information to a third party for the purpose of providing the consumer with a financial incentive, sale, or other discount if the business obtains the express consent of the consumer to sell the information to the specific third party."

In other words, information of consumers can be misused by companies by offering some money to the consumers. The word 'consent' is present in the act but including financial incentives implies that the consumer is forced to share his data for saving money.

Assembly bill 873 reads as under

"The act excludes from the definition of personal information consumer information that is deidentified, or aggregate consumer information. The act defines "deidentified" to mean information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer."

This means that all information which is labelled as deidentified and not associated with any person can be shared by companies and massive data privacy violations can be made by companies.

Assembly bill 1416 reads as under

"Sell the personal information of a consumer who has opted-out of the sale of the consumer's personal information to another person for the sole purpose of detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity." "Provide a consumer's personal information to a government agency solely for the purposes of carrying out a government program."

The bill will have the same effect which was also caused by personal data protection bill of India. These data privacy violations by government and private individuals are legalized under the given bill. "The bill could clear the path for private companies such as the data brokers and surveillance corporations ... to collect, keep, and sell the personal information of Californians without giving them a meaningful choice in the matter," reads a statement from Sen. Hannah-Beth Jackson, chair of the Senate Judiciary Committee.

These amendments to the act weakened the stringent data protection law by creating exceptions to collect, use and sell consumers data by companies. The bill was compared with data protection law of European Union (EU) i.e. General Data Protection Laws (GDPR) but the time taken to enact CCPA is very less than the time taken to enact GDPR. The law has many loopholes because it was swooped in without proper discussion of its implications. The privacy definition given under this bill is so vast that it exceeds data protection and makes business difficult for companies. Thus, privacy legislations need to be of such a type that recognize criminal intent rather than to protect all data of consumers and making business impossible in the time of Globalization.

3.2 Russia

On May 1, 2019 Russian president Vladimir Putin signed a Sovereign Internet' Bill for Russia which aims to isolate the country's internet. The bill (No. 608767-7) amends the laws "On Communications" and "On Information, Information Technologies and Information Protection". The law is not in effect at the time when this paper is being written and will go into effect in first week of November. The measures include creating technology to monitor internet routing through Roscomnadzor, the Kremlin's Internet censor and to steer Russian internet traffic away from foreign servers i.e.to create a national domain name system (DNS), ostensibly to prevent a foreign country from shutting it down. If Russia builds a workable version and switches it on, traffic would not enter or leave Russia's borders. In effect, it means turning on a standalone Russian internet, disconnected from the rest of the world.

This will allow the government, for example, to redirect searches from independent news organizations to pro-government websites. A similar law was passed in March with objective of allowing jail people who insult or defame government officials online. Under this many people were arrested for opinions against government officials. No country has ever tried to build its own internet architecture before. Even China, the world leader when it comes to internet censorship, has built its "Great Firewall" on the existing global DNS—it filters traffic, but is still part of the same worldwide addressing system. [12] The bill also gives authorities to block sites which they think are not

appropriate for citizens of Russia.
Under this law internet providers in Russia will also have to give centralised traffic control to the Government. Sovereign law of Russia can be majorly be related to the Indian notification which was issued by the Indian Government recently and is also stated above. The notification stated that ten Government agencies can spy on data of Indian citizens which is also similar in case of Russia where Kremlin (government's internet regulation agency) can spy on the country's online activity. The protest against the government's decision could be seen in citizens of Russia when the famous 'telegram' app was banned by the Russian authorities as it violated government's restriction. Despite ban on the app many users bypassed the restriction to use the app.
Now, coming to criticisms or loopholes in the above bill which was protested widely across Russia. This bill will impact data privacy the most among all the laws discussed in this paper because it is quite clear from Russia's laws in recent years that it wants to maximize government control and censorship over the internet. Many privacy advocates have objected to the law as it will increase the states surveillance and control of information. The isolation of internet of Russia will also have a large effect on the economy of Russia as the network required for these services will be disrupted. This bill will have a bad effect in long run as the majority of citizens will start using VPN.
This in turn will lead to large workload for Russian authorities and will start a game of cat and mouse between authorities and citizens which is not a good trait for a democracy. This isolation will in turn effect the global interaction of Russian and limit the flow of ideas in Russia. The government can ensure that nothing which is against decisions of the state goes on the internet and will manipulate the data. Human Rights Watch issued the following statement: "These proposals are very broad, overly vague, and vest in the government unlimited and opaque discretion to define threats. They carry serious risks to the security and safety of commercial and private users and undermine the right to freedom of expression, access to information and media freedom."
In this era of globalisation this step is being seen a step backward in developing state of mind of Russian citizens. This move can also be seen as a step to counter domestic political opposition. This legislation is not all bad as the rationale behind enacting such a law was to protect Russia from any foreign intervention or cyber-attack. This move was taken after security threat from US of a possible cut of internet from rest of the world as the DNS server is under US control. But this step is gross violation of human rights of citizens of Russia as one should have the right of watching what he wants to unless it is a threat to security of the state or immoral for society to see.

3.3 Spain
EU's GDPR which came into being on May 25, 2018 is also applicable on Spain as it is a part of EU. In December 2018 Spain introduced Spain Data Protection act under GDPR. EU's GDPR is a widely praised legislation and secures almost all aspects of data protection of people of EU without violation of data privacy of its citizens (reason GDPR is not listed in this paper). It is a well drafted legislation and a ideal Act to be looked onto by other countries when enacting a data privacy act. But while enacting GDPR Spain introduced a new article 58 in its Spanish Electoral System Act (LOREG). Art. 58 states:
"Use of technological means and personal data in electoral activities:

1. The collection of personal data relating to the political opinions of individuals carried out by political parties in the performance of their electoral activities shall be deemed to be in the public interest.
2. Political parties, coalitions and electoral groupings may use personal data obtained from websites and other publicly accessible sources in the performance of political activities during the electoral period."

This amendment was passed in parliament with 220 votes. "That is, political parties have given themselves legal authority to collect personal data regarding the political ideology of citizens (i.e. a special category of data which require, by legal imperative, a higher level of protection) from social networks and the Internet to personalize electoral propaganda." [13] Elections in recent times are contested less on ground and more on internet. This is the main reason why this step is seen as a strategy by politicians to impact the coming elections of EU and its member countries.
GDPR also has a similar article i.e. 56 on which art. 58 of Spanish electoral act is based. Recital 56 states "where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established." In this article two things are clearly mentioned which are missing from Art. 58 of LOREG. First, there is no definition of public interest in LOREG whereas public interest is clearly defined in GDPR. Second in GDPR it is clearly explained when data of citizens will be collected but in LOREG there is no mention of reasoning for which the data can be collected, it is simply stated that collection of data will take place in electoral process.
Similar laws were also introduced in which along with GDPR, amendments were introduced to create loopholes in GDPR for political parties declining their citizen's right to privacy. The laws enacted recently containing these loopholes viz. Romanian data protection law and UK DPA. The same concerns which were raised at the time of amendment of LOREG were raised at the time of enactment of these law by various civil society organizations and NGO's. The UK law further specifies that political opinion will be revealed without consent. This provision will lead to targeting of social media accounts and banning of those accounts which go against the ruling party.
Citizens of Spain have a right to data protection both under the Constitution of Spain in Article 18(4) and under Article 8 of the Charter of Rights of the European Union. The above amendment violated both the articles and are therefore unconstitutional.

4. Conclusion
The purpose of the above laws was to ensure data privacy to citizens of the country in which they were enacted. But enactment of these laws faced many challenges because of

different and obvious reasons. First being the very legislature constituting politicians from different party's tried to induct loopholes for their electoral process while enacting them. Second, as cybercrime is on rise digital surveillance is also on rise which is also necessary but the misuse of this data is a major issue when one takes digital surveillance into account. Third there is no data protection authority which can keep a check on what data is being used by the government through decryption. Fourth, many data protection laws have imposed censorship on data of citizens which limits new ideas as well as leads to unrest among citizens. Finally, some laws were biased towards business giving them an upper hand in handling of data privacy. Whereas almost all recent data privacy violations have taken place in large tech companies it be Facebook controversy or LinkedIn controversy of 2016 and many more.

4.1 Suggestions

Terms and conditions play a vital role in giving consent while using any service on internet. These terms and conditions include many provisions which are gross violation of privacy of individuals but are not treated violative because consent of consumers are obtained on those provisions. This happens because these provisions are not read by individuals using the service as a large amount of information is present in the consent form. This can be get ridded of by highlighting information which can be considered sensitive from the view of privacy of consumer. Considering recent laws one common conclusion can be drawn and i.e. almost all data protection laws have loopholes related to data privacy of citizens but GDPR can be considered an ideal law for laws enacted or to be enacted in other parts of the world specifically in terms of privacy violations.

5. References

1. Definition of "data" from the Cambridge Business English Dictionary © Cambridge University Press
2. Definition of "data protection" from the Cambridge Business English Dictionary © Cambridge University Press
3. Anon., n.d. European Data Protection Supervisor (8 August 2019) https://edps.europa.eu/data-protection_en
4. Puttaswamy KS. V Union of India, 2018 SCC Online SC 1642
5. Information technology act, 2000.
6. Sriram J. SC strikes down 'draconian' Section 66A, New Delhi: The Hindu, 2015.
7. Agarwal S. Justice BN Srikrishna to head Committee for data protection framework, New Delhi: The Economic Times, 2017.
8. QC HT. Inforrm's Blog. Available at: https://inforrm. Org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/ [Accessed 1 September 2019], 2017.
9. Merwin R. All you wanted to know about Personal Data Protection Bill 2018. Available at: https://www.thehindubusinessline.com/opinion/columns/slate/all-you-wanted-to-know-about/article24617362.Ece [Accessed 2 September 2019].
10. Anon. Council on Foreign Relations, 2018. Available at: https://www.cfr.org/blog/three-problems-indias-draft-data-protection-bill [Accessed 2 September 2019].
11. Ingram CFAD, 2019. CNBC. Available at: https://www.cnbc.com/2019/05/14/california-consumer-privacy-act-could-change-the-internet-in-the-us.html [Accessed 8 September 2019].
12. Bremmer I. 2019. TIME. Available at: https://time. Com/5578737/the-quick-read-about-russias-new-internet-law/ [Accessed 24 September 2019].
13. González, EG. The Good, The Bad And The Ugly: Spanish Electoral System Act: A Tale With A Happy Ending, 2019; 6:10. Retrieved from Secuoya: https:// secuoyagroup.com/2019/06/the-good-the-bad-and-the-ugly-spanish-electoral-system-act-a-tale-with-a-happy-ending/