Centre for Society and Policy
Indian Institute of Science

OVERVIEW OF PERSONAL DATA PROTECTION LAWS, REGULATIONS AND POLICIES GLOBALLY

By

Rahul Patil

Anjula Gurtoo

24 August 2020

INDIAN INSTITUTE OF SCIENCE

BANGALORE

1. Abstract

Data is an architect for new socio-economic alignments in the 21st Century. Data has become a part of everyone's life, just like Oil and Steel became in the past Century. Governments, policymakers, and policy researchers around the globe are not far behind in resonating with advancements in the data economy that is now one of the fastest-growing technological areas. Since the beginning of the present millennium, the sense of regulating the data economy's engagement with socio-economic dimensions has started emerging strongly. Governments started revisiting their regulations for improvisation to keep their relevancy intact. The process accelerated in the 2010s when governments came out with remarkable initiatives and policy instruments to balance data access and privacy rights. Though, it needs highlighting that there is still much room to improve upon various provisions of these guiding instruments considering the technological developments on the technological front. This report discusses a range of provisions for personal data protection across intra-national legislation, regulations, policy frameworks, and some international arrangements as cross-border facilitation for the free flow of personal data.

Citation: Patil, R. and Gurtoo, A. (2020). Overview of Personal Data Protection Laws, Regulations and Policies Globally. IISc CSP Working Paper Series. 1C/07/2020.

Table of Contents

2. Introduction

Globally, countries are proactively searching for options to protect their citizens and information. They want to fit themselves in a rapidly evolving digital world. Since the

beginning, countries have opted for a route of legislation to protect the flow of public/private information, maintaining privacy and security concerns and rights assigned to the citizens regarding their information. However, these provisions vary with different degrees of strictness across countries, either in the form of dedicated data regulation or in the parts of legislation such as sector-wise, state-wise, based on the age of the citizens or type of organisation, and so on.

Many countries apex level instruments recognise privacy or private life as a fundamental right of the citizens as the Indian Constitution, under Article 21, designates the fundamental right to life & liberty to its citizen (Indian Constitution, 1950), European Convention on Human Rights proclaims the right to respect for private and family life as early as 1950 (ECHR, 1950), and China highlights right of reputation or right of privacy under General Principles of Civil Law (PRC, 1986) and the Tort Liability Law (PRC, 2009), on the other hand, countries started enacting legislation to realise these fundamental right to citizens like Australia's effort to acknowledge privacy as a fundamental right through the enactment of the Privacy Act (Privacy Act, 1988) in 1988.

3. Methodology

The present report focuses on the global grey literature released by governments and their agencies to capture the national priorities in the personal data economy. Leading countries and regions were identified through a survey of the scholarly literature. On identification of the leading regions, Government reports, legislation, regulations, and policy documents were mined from various government sources such as the websites of ministries, departments, parliaments, etc. Dedicated legislative databases and databanks were found to be useful for data mining. Search has been restricted to the personal data protection bills, regulations/legislation, case laws, frameworks, and guidelines for which keywords were identified accordingly. The search was optimised to prior (repealed), present (active), and proposed (bills/non-enacted) provisions and was not limited with respect to timelines.

On data retrieval, the landscaping of documents was carried out in the spreadsheets, which mainly included mapping important provisions and their features in respective counties. These were further carved out in the form of the present report.

4. Worldwide Regulations on Personal Data Protection

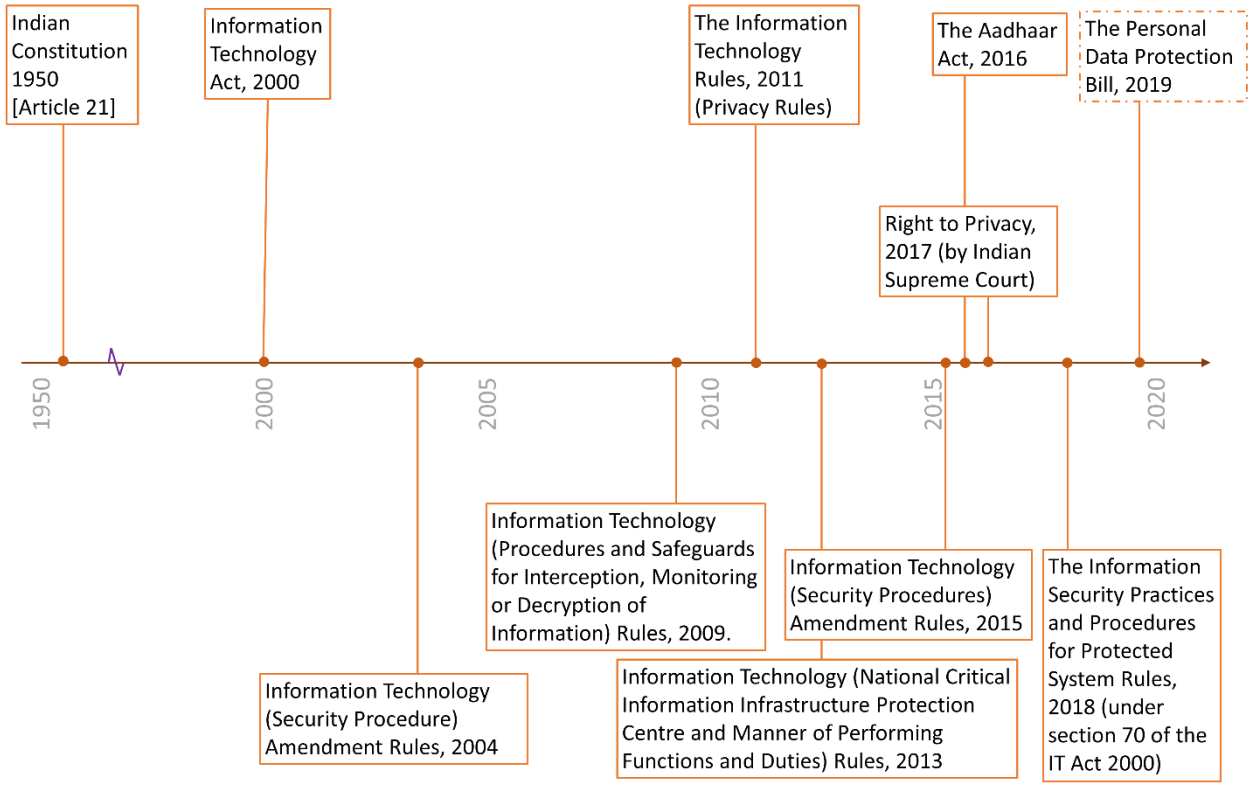
4.1 Title Case: India

India has no single comprehensive legislation addressing data protection. Instead, a range of laws and their abiding rules extend protection to personal or private information through sector-specific laws. However, emerging economies are recently stepping towards enacting comprehensive legislation governing data protection, and India is no exception.

In a landmark case, **Justice K. S. Puttaswamy (Retd.) v. Union of India**, a Constitutional Bench of nine judges of the Supreme Court of India unanimously upheld the right to privacy as a fundamental right on August 24, 2017 (Justice KS Puttaswamy (Retd.) Vs. Union of India and Ors, 2017). This judgment paved the way for several interventions, including the foundation of India's proposed Personal Data Protection Bill 2019 (PDP Bill, 2019). The formulation of this Bill was proposed based on the suggestions devised in the comprehensive report (CEDPF Report, 2018) submitted, on July 27, 2018, by a specially appointed Committee of Experts on a Data Protection Framework for India by the Government of India to make specific suggestions on the principles underlying a data protection. On December 11, 2019, the Bill was introduced in the Lower House of the Parliament and later referred for review to a thirty-member Joint Committee (Lok Sabha, 2019) of the members of Parliament of India.

Currently, data protection in India is being addressed by a bunch of laws and their abiding rules, mainly involving **the Information Technology Act, 2000,** enacted on 09 June 2000. and its privacy rules, **the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules**, released on 11 April 2011. Primarily, it governs the issues regarding cyber-crime and the liability of internet platforms. The provisions like section 43A of the IT Act allow compensation in case of damages caused by a breach of security practices in protecting sensitive personal data. Additionally, the recently released privacy rules distinguish 'personal information' from 'sensitive personal information. They expect corporate entities to comply with the prescribed procedures while collecting, processing, and storing personal information, including sensitive personal information. These provisions tried to address the elements highlighted in the Supreme Court Judgement: privacy is an integral part of an individual's identity, and informational privacy is a subset of it.

Diagram 1: Timeline for Indian Regulations relevant to Personal Data Protection



The report submitted by a specially appointed Committee by the Government of India also prescribed amendments to the two acts: the Aadhaar Act (Aadhaar, 2016) and the RTI Act (RTI, 2005). It also highlights the allied laws as an impact on the enactment of the proposed law considering the overlap of the provisions. These allied laws included a list of 50 statutes and regulations (CEDPF Report, 2018).

The proposed Act is increasingly being compared to the European Union's General Data Protection Regulation – EU Directive GDPR (discussed subsequently in the article). The importance which can be highlighted here is that GDPR is an amendment to the existing Data Protection Directive of 1995. On the other hand, the proposed Act has no such precursor in India. This might raise the cost of compliance and data protection obligations (Burman, A., 2019). Bailey and Parsheera (2018) advised systematic economic analysis of the proposed bill. Enactment of the proposed Bill will directly impact the Indian economy, such as increased expenditure due to mandatory data protection practices, or indirectly affect the rate of research, development, and innovation.

4.2 Other leading regions

4.2.1 Brazil

Brazil enacted **Lei Geral de Proteção de Dados [LGPD]** – General Data Protection Law as a Federal Law no. 13709/2018 on 15 August 2018 (Brazilian Internet Law, 2018). This law applies to any business or organization that processes the personal data of people in Brazil regardless of where that business or organization itself might be located - i.e., extraterritorial application. It unifies the over 40 statutes that currently govern personal data, both online and offline, by replacing certain regulations and supplementing others. Article 18 of the GDPL enlists nine fundamental rights to the data subjects. LGPD adopted a broader definition of personal data as compared to the GDPR. LGPD and GDPR vary on the points such as - stricter requirements of data protection officers (applicable to every organisation handling Brazilians' data). LGPD enlists ten lawful bases for data processing. LGPD does not give a deadline (as in the case of the GDPR, i.e., 72 hours) for reporting security breaches by organisations to the Data Protection Authorities. Fines are less severe in LGPD (2% of a private legal entity) as compared to EU's GDPR (up to €20 million or 4% of annual global revenue) (GDPR.EU webpage).

Another act, **the Brazilian Civil Rights Framework for the Internet**, better known as the Brazilian Internet Act [Federal Law no. 12965/2014] enacted on 23 April 2014, relates to the security and the processing of personal data and other obligations on service providers, networks and applications providers, as well as rights of Internet users.

4.2.2 China

A right of reputation or right of privacy is generally considered under the umbrella of **the General Principles of Civil Law** and **the Tort Liability Law** and considered the pavement for data protection rights.

Recently, China has actively intervened in the field of information security. It includes the **PRC Cybersecurity Law** which was enacted on June 1, 2017 (PRC Cybersecurity Law 2017), the National Standard of Information Security Technology – **Personal Information Security (PIS) Specification** effective from May 1, 2018 (PRC PISS, 2018); and Guidelines on Internet Personal Information Security Protection, effective from April 19, 2019 (Sacks S., 2018 et al.). **Legislation on personal data protection and security** by the Legal Committee of the National

People's Congress Standing Committee is set to be enacted in 2020. It's seen that China previously followed the US approach in data protection; however, it later aligned its enactments, such as Cybersecurity Law and the PIS Specification, similar to European standards (Pernot-Leplay, E., 2020).

4.2.3 European Union

Article 8 of **the Convention of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms** establishes the right to respect for private and family life. **The Council of Europe Convention 108 of 28 January 1981** (CEC, 1981) advocates for protecting individuals related to the automatic processing of personal data. It deals with citizens' data protection rights, fundamental freedoms, and the right to privacy.

Article 7 and 8 of **the EU Charter of Fundamental Rights** (CFR EU 2012) - 2007/C 303/01 primarily empower citizens of EU's member states with data privacy and personal data, in particular. Article 7 advocates for respect for private and family life, and Article 8 protects personal data. It emphasizes the right to the protection of personal data, access to personal data collected by others and the right to rectify the same, and compliance with the rules to be controlled by an independent authority.

European Union's comprehensive data security and protection instrument, the General Data Protection Regulation, i.e., GDPR (EU Directive 2016/679), entered into force on 24 May 2016 and has been applied since 25 May 2018 (GDPR, 2016). This directive repealed the Data Protection Directive (Directive 95/46/EC) of the European Commission and Council of 24 October 1995 (EP Directive, 1995). Previously, the European Commission in January 2012 proposed a comprehensive reform of data protection rules to increase users' control of their data and cut business costs (EC Press Release, 2012). As a part of several deliberations within the European Commission, the European Parliament in December 2015 concluded the requirement of modern and harmonized new data protection rules across the EU. It was considered a significant step towards implementing Digital Single Market Strategy as a priority for 2019-24 (EC 2019).

The General Data Protection Regulation, i.e., GDPR, deals with the protection of individuals related to the processing of personal data and the free movement of the same. Chapter II of the

GDPR entails principles related to the processing of personal data (Article 5), the lawfulness of processing (Article 6), conditions for consent (Article 7), requirements in particular for child's consent (Article 8), conditions for special categories of data focusing on inclusive nature (Article 9), conditions for personal data related to criminal convictions and offenses (Article 10), and conditions for the processing of data which does not require identification.

These principles outline guidelines for processing of data such as adopting lawfulness, fairness and transparency in personal data protection; collected data should be rightfully processed with the predetermined limitation; data minimisation is advised considering the adequacy and relevancy of the requirement of processing; personal data should no longer be stored than necessary; integrity and confidentiality should be adopted in data processing to avoid unauthorised or unlawful processing; controller shall be able to demonstrate the individual has consented; if the consent has to be sought for multiple matters, they should be distinguishable; allow right to withdraw consent should not affect lawfulness of data processing; consent of the child should be considered valid at the age of at least 16 years otherwise it's parental responsibility, members states may lower the age limit but not below 13 years; and prohibition of processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, the processing of genetic data, biometric data, health data or of sexual orientation, and data related to criminal convictions and offences.

Regulation (EU) 2018/1725 lays down the data protection obligations, transparency, and accessibility of practices in the Union institutions, bodies, offices, and agencies while processing personal data and developing new policies (EU Regulation, 2018). This regulation also advocates for the enhanced role of data protection officers within the EU. It adopted principles aligned with the GDPR and repealed Regulation (EC) 45/2001.

Along the same line, another EU Directive 2016/680, i.e., **The Data Protection Law Enforcement Directive,** deals with the protection of individuals in relation to the processing of personal data by the competent authorities for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties along with the free movement the data related to it. This directive repealed Council Framework Decision 2008/977/JHA of 27 November 2008.

On the other hand, the EU has recently brought a range of sector-specific laws. **Directive (EU) 2016/681,** of which Article 13 deals with the protection of personal data such as the use of

passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime (EP Directive 2016. **Regulation (EU) 2016/794** of which Chapter VI (on data protection safeguards) deals with the European Union Agency for Law Enforcement Cooperation - Europol (EU Regulation 2016). Chapter VIII (on data protection) of **Council Regulation (EU) 2017/1939** deals with the deals with implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office – EPPO (EU Council Regulation 2017).

4.2.4 Indonesia

Recently, in 2016, the **Electronic Information and Transactions (EIT) Law Amendment** (Law No. 19 of 2016) were approved by Indonesia to repeal Electronic Information and Transactions (EIT Law - Law No. 11 of 2008). The **EIT Law**'s Article 26 entails the right to enjoy a private life, free of any disturbance; the right to communicate with other people without any espionage; and the right to monitor the access of information about a person's personal life and data. On the other hand, it does not state the definition of personal data.

Amendments to the 2008 EIT Law are not significantly different, whereas the amendments include defining electronic system provider, allotment of right to be forgotten, and government's right to terminate access. On the other hand, some of the provisions related to criminal sanctions are relaxed. Violation related to the defamation through electronic information had a maximum of 6-year imprisonment and/or a maximum fine of IDR 1 billion, which is relaxed to the 4-year imprisonment and/or maximum fine up to 750 million. The same criminal sanctions are applied in amended law for the violation regarding threats of violence and frightening information, which used to be a maximum of 12-year imprisonment and/or a maximum fine of IDR 2 billion (Molina K, 2016).

Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (Reg. 71 or GR 71) was developed as an amendment to the Government Regulation No. 82 of 2012 (GR 82). However, a series of deliberation and changes extended, leading to the repealing of GR82. The new regulations have provisions such as a more recent definition for public and private electronic system operators, new data localization requirements for public electronic system operators, provisions for the deletion of electronic

data, provisions on electronic certificates and electronic reliability certificates, a new scope of electronic certification services., etc. The GR82 failed to personal data.

Other than these**,** Indonesia enacted **the Minister of Communications & Informatics Regulation** No. 20 of 2016 (MOCI Regulation or MOCI Reg) deals with the protection of personal data in an electronic system; **the Telecommunications Law** (Law No. 36 of 1999) which prohibits tapping of information transmitted through telecommunications network (Article 40) and adoption of confidentiality by telecommunications services operator related to any information transmitted or received by a telecommunications service (Article 42); **the Law No. 14 of 2008** enacted on 30 April 2008 regarding disclosure of public information which prohibits disclosure of information relating to personal rights by public bodies (Article 6) and prohibits the disclosure of private information of any person (Article 17); **the Law 7 of 1992** as an amendment to Law 10 of 1998 & Law 8 of 1995 better known as Capital Markets Law which is applicable to individuals as well as corporate data; and **the Financial Services Authority Regulation No. 38/POJK.03/2016** relates to the implementation of risk management in the use of information technology by the banks where customer data transfer requires prior approval from the financial services authority.

Recently, the Protection of Private Personal Data Bill has been under consideration in Indonesia, submitted through Presidential Letter No. R-05/Pres/01/2020 to House of Representatives on 24 January 2020, the copy of which is only available in Indonesian.

4.2.5 Japan

Japan recently amended [Act no. 57] the **Act on the Protection of Personal Information** (APPI) entered into force on 30 May 2017, whereas the prior act was enacted on 30 May 2003 and came into force in 2005 (PIP Commission, 2016). This act authorised the establishment of the Personal Information Protection Commission (PPC), which governs privacy protection issues. Previously, until the enforcement of the amendment of the APPI, Japan's legal framework had field-specific guidelines and Chapter IV-VI of prior APPI for private business operators, whereas two acts for the public sector, including the Act on the Protection of Personal Information Held by Administrative Organs for the national government and Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc.

Chapters I to III of the prior APPI were responsible for a basic policy protecting personal information.

The amended APPI provides a more explicit definition of Personal Information and includes fingerprint data, facial recognition data, passport number, driver's license number, and individual numbers other than name, address, and date of birth. A newer definition of sensitive personal data is extended to race, religion, medical history, and personal information, which has the potential to bring about unjustifiable discrimination or prejudice. It sets rules for the utilisation of de-identified information, which involve two conditions, i.e., making information unidentifiable to the individual and prohibiting the restoration of personal information. The act sets three types of personal data transfer to foreign parties if prior consent has been sought for such data transfer, or the party from foreign considers personal data protection regulations equivalent to Japan or standards set by the PPC. The act also has provisions for extraterritorial application and cooperation by the PPC in cross-border enforcement. To avoid improper use of personal information, PPC can trace the flow of personal information across networks.

4.2.6 The United States of America

The United States of America hosts a patchwork of federal and state legislation, sector-specific, and cross-sector legislation in contrast to European's comprehensive General Data Protection Regulation, GDPR. Organisations handling the information of the United States citizens need to comply with requirements of federal as well as state laws. The federal and state laws are applied as a set of laws and not as exclusive of one another. Almost all the states have enacted the data protection regulation in some form. State Attorney General has the right to enforce federal and state laws.

Federal laws focus on data protection based on industry or data types, whereas states have enacted breach notifications laws and data security laws. In these laws, the definitions of personal and sensitive personal data vary, e.g., in Federal FTCA and California States' CCPA (both discussed follow).

The Federal Trade Commission Act of 1914 (FTCA, 1914), better known as FTCA, deals with the unfair or deceptive methods of competition and unfair acts or practices affecting commerce. It empowers the US Federal Trade Commission (US FTC), an authority against the

practices mentioned above, which include deceptive practices such as inadequate protection measures for citizen's information (FTC, 2004) and unauthorised access or disclosure of consumers without prior consent (FTC, 2000).

The Health Insurance Portability and Accountability Act of 1996, abbreviated as HIPAA (Kennedy–Kassebaum Act) (HIPPA, 1996) and The Health Information Technology for Economic and Clinical Health Act (HITECHA, 2009) – HITECH Act are the sector-specific federal law for data protection. HIPAA requires the organisation involved in health data to comply with provisions of collection, maintenance, usage, or disclosure of personal health information. The disclosure of such information is considered unauthorised except under specific circumstances or where authorized by the patient or participant. The HITECH Act expands the scope of HIPAA's provisions to concerned organisations' business associates, e.g., non-profit affiliates.

The Family Educational Rights and Privacy Act of 1974 (FERPA, 1974) was enacted to govern the flow and protection of data related to students' educational records. This law directs the institutions funded by the US Department of Education. It is mandatory for the organisation collecting or sharing education information to take consent from the eligible students or their guardians otherwise regarding the release of personal information enclosed within it. Such consent can also be sought through public notices; however, sufficient time needs to be given to the respondents to get back. The concerned organisation should keep a log of entities requesting and obtaining students' education and personal data.

The Children's Online Privacy Protection Act of 1998 (COPPA, 1998) – COPPA was enacted to direct operators of a website dealing with the collection, usage, and disclosure of children's personal information and aims to protect children under the age of thirteen. It is mandatory for organisations involved in such practices to seek consent from the parent regarding mentioned practices.

Non-Solicited Pornography and Marketing Act of 2003 (NPMA, 2003) - CAN-SPAM Act is a regulation enforced to curtail misleading or deceptive information sent through commercial or promotional emails. The law requires senders to cite their valid physical addresses in such communications and provides provisions to opt-out of such mail lists, whereas it's mandatory for senders to respect this decision.

The Financial Services Modernization Act of 1999 (FSMA, 1999), better known as The Gramm-Leach-Bliley Act – GLBA, applies to financial organisations and requires data protection practices to be followed, which involve maintaining the privacy, security, & confidentiality of non-public personal information of customers. This law also extends to financial organisations such as federal functional regulators, state insurance authorities, or the FTC itself. They are directed to share their privacy policy annually with all the customers or clients. Enactment of the GLBA repealed prior Glass–Steagall Act. Another legislation, **the Fair Credit Reporting Act** (FCRA 1970) – **FCRA** applies to consumer reporting agencies to promote the accuracy, fairness, and privacy of consumer information. In particular, this law extends the provisions of GLBA to financial organisations outside its purview, e.g., non-profit agencies. It is mandatory under the law to notify the concerned person about the sharing of their information as well as offer an opportunity to opt-out from sharing it with others which will be effective for five years.

Meanwhile, in 2004, **Payment Card Industry Data Security Standard** (PCI DSS, 2018) has also launched to ensure the handling of sensitive credit card information. This standard needs to be followed by all the entities dealing with payment card processing and storing, using, or sharing data. It should be noted that there is no private right of action under the GLBA statute, which government regulators may enforce. On the other hand, FCRA provides a private right of action for wilful noncompliance, knowing noncompliance, and negligent noncompliance.

The United States enacted the law, **Clarifying Lawful Overseas Use of Data Act** (CLOUD Act, 2018) in 2018, which provides trans-border access to data in criminal law enforcement investigations. This act permits federal officials to access foreign stored data and creates executive arrangements for foreign access to US-based data.

On the front of states' laws, States like California, Massachusetts, New York, and the District of Columbia have some comprehensive legislation, such as the recently enacted **California Consumer Privacy Act (CCPA).** Though enacted in 2018, it's effective from 1 January 2020 in California. It advocates for ownership of personal data to the consumer, allows them to know about the collection of their information by various entities, and allows the right to delete such information and opt out of such practices. California State also amended the California State is **Online Privacy Protection Act of 2003** (CalOPPA) in 2013, which prompted operators of commercial websites or online services to include privacy policies. Other notable acts enacted

by California State include the **Financial Information Privacy Act** (CFIPA, 2004), which intends to provide greater privacy protections than those provided in the federal Gramm-Leach-Bliley Act, and the **California Shine the Light Law** (CSLL 2005) applies to the organisation sharing data for direct marketing purposes excluding the non-profit organisations disclosing data for charitable contributions. The organisations need to avail the privacy policies detailing data sharing practices free of cost on request of any Californian resident.

The New York State has enacted two notable data protection laws. **The States' Attorney General particularly enforces Information Security Breach and Notification Act.** The law demands immediate disclosure of a breach of the security of the system by the organisations, along with the approximate number of people affected by the breach. Another act, **the Social Security Number Protection Law,** strictly prohibits public disclosure of unencrypted social security numbers or their printing on the cards, tags, products, services, or over the internet unless required by law.

Similarly, the District of Columbia (DC)'s **Consumer Personal Information Security Breach Notification Act** applies to businesses conducted in the DC that own or license computerised or electronic data. This law can be enforced by private individuals affected by the security breach and the state attorney general. The organisations need to notify the affected individual mandatorily.

Recently, Senator Warren unveiled a bill (Warren E, 2019) that aims to **expand criminal liability** where negligent executives of giant corporations might be criminally accountable if they repeatedly violet federal law.

5. Discussion and Conclusion

Worldwide, governments and policymakers have actively shown concerns about regulating the data economy. Most governments and the judiciary have prioritised privacy protection. Since the beginning, the privacy of the country's citizens has been respected and is further incorporated into the respective legislations and iterated by apex courts of the countries, as seen in the case of Justice KS Puttaswamy (Retd.) Vs. Union of India and Ors in India in 2017.

Governments are either enacting new regulations or amending their existing legislative framework altogether, as seen in the case of the General Data Protection Regulation in the EU

in 2016, which was the amendment of Directive 95/46/EC (General Data Protection Regulation, 1995), whereas newly bought forward EU Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime.

Altogether, these policy instruments have provisions for the personal data protection, free flow of personal information, assignment of data regulation authority and personnel in various capacities, data localisation requirements within certain geographical locations, grant of the consent of the natural person to whom data belongs, data portability, right to erase, and so on. Various Governments globally are still in the process of adopting some of the abovementioned provisions in their national legislations. Policy researchers are carrying out assessments of these processes and provisions undertaken. It has been observed that the provisions such as portability rights and the right to erase have been adopted in limited aspects, whereas some the policymakers have raised queries over the provisions of data protection regulations in China and Taiwan, giving more control to the governments regarding the flow of information rather than protection of individual's data privacy.

References

Aadhaar, 2016. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 - Aadhaar Act https://www.indiacode.nic.in/bitstream/123456789/2160/1/201618.pdf - enacted on 11 March 2016

Aljazeera, 2018. https://www.aljazeera.com/news/2018/06/vietnam-cybersecurity-law-devastating-blow-freedom-amnesty-180613074931697.html

Amnesty, 2018. https://www.amnesty.org/en/latest/news/2018/06/viet-nam-cybersecurity-law-devastating-blow-freedom-of-expression/

Bailey, R. and Parsheera, S. 2018. Questioning the Means and Ends. NIPFP Working Paper Series No. 242, https://www.nipfp.org.in/media/medialibrary/2018/10/WP_2018_242.pdf.

Brazilian Internet Law, 2018. https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf

Burman, A., 2019. Will a GDPR-Style Data Protection Law Work For India? Carnegie India. https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113

CEC, 1981. The Council of Europe Convention 108 of 28 January 1981, https://www.coe.int/en/web/data-protection/convention108-and-protocol

CEDPF Report, 2018. A Free and Fair Digital Economy - Protecting Privacy, Empowering Indians. A report of a Committee of Experts on a Data Protection Framework for India chaired by Justice B.N. Srikrishna – dated 27 July 2018 https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf

CEDPF Report, 2018. Annexure C of 'Free and Fair Digital Economy - Protecting Privacy, Empowering Indians' – A report of a Committee of Experts on a Data Protection Framework for India chaired by Justice B.N. Srikrishna – dated 27 July 2018 https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf

CFIPA, 2004. California Financial Information Privacy Act, effective from 01 January 2004 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=4051.&lawCode=FIN

CFR EU, 2012. Charter of Fundamental Rights of the European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

CLOUD Act, 2018. Clarifying Lawful Overseas Use of Data Act – enacted by the passing of the Consolidated Appropriations Act, 2018, PL 115-141 – With effective from 23 March 2018 https://epic.org/privacy/cloud-act/cloud-act-text.pdf

COPPA, 1998.15 U.S.C. §§ 1681, The Children's Online Privacy Protection Act of 1998 enacted on 21 October 1998 https://www.govinfo.gov/content/pkg/PLAW-105publ277/pdf/PLAW-105publ277.pdf

CSLL, 2005. California Shine the Light Law, with effective from 01 January 2005 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV

EC, 2019. Ursula von der Leyen. A Union that strives for more - My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024. https://ec.europa.eu/info/strategy/priorities-2019-2024

EC Press Release, 2012. https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46

ECHR, 1950. Article 8 of European Convention on Human Rights (ECHR) of 4 November 1950, https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

EP Directive, 1995. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

EP Directive, 2016. EP Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595439074640&uri=CELEX:32016L0681

EU Council Regulation, 2017. EU Council Regulation implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO') https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595439251335&uri=CELEX:32017R1939

EU Regulation, 2016. EU Regulation on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595439115093&uri=CELEX:32016R0794

EU Regulation, 2018. EU Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1595437874853&uri=CELEX:32018R1725

FCRA, 1970. 15 U.S.C. § 1681, The Fair Credit Reporting Act (FCRA), with effective from 26 October 1970 https://www.govinfo.gov/content/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf

FERPA, 1974. 20 USC § 1232g, The Family Educational Rights and Privacy Act of 1974 enacted on 21 February 1974 https://www.law.cornell.edu/uscode/text/20/1232g

FSMA, 1999. The Financial Services Modernization Act of 1999 or the Gramm-Leach-Bliley Act (GLB Act or GLBA), with effective from 12 November 1999 https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

FTC, 2000. FTC vs. Rennert, Sandra L., et al. FTC Matter/File Number: 992 3245 docket available at https://www.ftc.gov/enforcement/cases-proceedings/992-3245/rennert-sandra-l-et-al

FTC, 2004. *In the Matter of Petco Animal Supplies, Inc*., FTC File No. 032-3221 (2004) – Refer to Decision and Order at https://www.ftc.gov/sites/default/files/documents/cases/2005/03/050308do0323221.pdf https://www.ftc.gov/enforcement/cases-proceedings/032-3221/petco-animal-supplies-inc-th-matter

FTCA, 1914. The Federal Trade Commission Act of 1914 enacted on 26 September 1914 https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim

GDPR, 2016. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

GDPR.EU webpage, https://gdpr.eu/gdpr-vs-lgpd/

HIPPA, 1996. 45 C.F.R. § 160.102 or § 160.104, The Health Insurance Portability and Accountability Act of 1996 enacted on 28 March 1996 https://www.cdc.gov/phlp/publications/topic/hipaa.html

HITECHA, 2009. 42 U.S.C. §§ 300jj, The Health Information Technology for Economic and Clinical Health Act, abbreviated HITECH Act, enacted under Title XIII of the

American Recovery and Reinvestment Act of 2009 https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf

ICNUDP Act, 2016. THE ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND DATA PROTECTION, ETC. https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830760&fileSn=0

Indian Constitution, 1950. Article 21 of the Indian Constitution, Protection of life and personal liberty (as of 9th November 2015), http://legislative.gov.in/sites/default/files/coi-4March2016.pdf

Justice KS Puttaswamy (Retd.) Vs. Union of India and Ors, 2017. Writ Petition No. 494/ 2012, dated 24 August 2017 https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_judgement_24-aug-2017.pdf

Lok Sabha, 2019. Joint Committee on the Personal Data Protection Bill, 2019 chaired by Smt. Meenakshi Lekhi constituted http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 – dated December 11, 2019

Molina K, 2016. Molina Kristao, 2016. Indonesian Electronic Information and Transactions Law Amended. White & Case. https://www.whitecase.com/publications/alert/indonesian-electronic-information-and-transactions-law-amended

NPMA, 2003. Non-Solicited Pornography and Marketing Act of 2003 enacted on 16 December 2003 https://www.law.cornell.edu/uscode/text/15/chapter-103

PCI DSS, 2018. Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

PDP Bill, 2019. India's Personal Data Protection Bill 2019, Introduced in the lower House of the Parliament on 11 December 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

Pernot-Leplay, E., 2020. Pernot-Leplay , Emmanuel, 2020. China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?, Penn State Journal of Law & International Affairs.Vol. 8, Iss. 1. https://elibrary.law.psu.edu/jlia/vol8/iss1/6 & https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia

PIP Commission, 2016. Personal Information Protection Commission, Japan. 2016 Amended Act on the Protection of Personal Information (Tentative Translation) https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

PIPA, 2016. Personal Information Protection Act. https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830758&fileSn=1&nttId=8186&toolVer=&toolCntKey_1=

PRC, 1986. General Principles of the Civil Law of the PRC adopted by presidential order on April 12 1986. https://www.ilo.org/dyn/natlex/docs/electronic/49688/108015/F2085571488/chn49688%20eng.pdf

PRC, 2009. Tort Law of the PRC adopted at the 12th session of the Standing Committee of the Eleventh National People's Congress on December 26, 2009, https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn136en.pdf

PRC Cybersecurity Law, 2017. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

PRC PISS, 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/

Privacy Act, 1988. Act No. 119 of 1988 with the date of assent 14 December 1988, https://www.legislation.gov.au/Details/C2020C00168 (amended as of Act No. 44, 2020; 29 May 2020)

RTI, 2005. The Right to Information Act, 2005 – enacted on 15 June 2005 and RTI Rules, 2012 (31 July 2012) https://www.indiacode.nic.in/bitstream/123456789/2065/1/200522.pdf

Sacks S., 2018 et al. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/public-security-ministry-aligns-chinese-data-protection-regime-draft-rules/

Vietnam, 2013. The 2013 Constitution of the Socialist Republic of Vietnam https://vietnamlawmagazine.vn/the-2013-constitution-of-the-socialist-republic-of-vietnam-4847.html

Vietnam, 2018a. https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf

Vietnam, 2018b. https://hethongphapluat.com/law-no-35-2018-qh14-dated-november-20-2018-amendments-to-some-articles-concerning-planning-of-37-laws.html

Warren E, 2019. https://www.warren.senate.gov/newsroom/press-releases/senator-warren-unveils-bill-to-expand-criminal-liability-to-negligent-executives-of-giant-corporations