International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Security and Trade, How Global Markets Are Shaped by Global Data Privacy and Cyber Legislations

Harish.R[1], Tejas.R[2]

[1,2]Student, Sastra University

Abstract

In this article we shall explore how digitalisation of global trade and commerce is affecting data privacy of consumers and what are the impacts of legislations that help in shaping e-commerce throughout the world and how are sellers and buyers impacted by it. We shall dive into the legal provisions mainly in India and present an analysis of how these legislations fulfill their purpose. In case of failure of lack of teeth in the law enforcement agencies to enforce laws regarding data privacy and cybersecurity. This article will also include how e-commerce giants comply with cyber security laws across the world and are they enough to prevent malpractice and fraud, both by hackers and by sellers themselves.

Chapter - I

Introduction

Cyberspace today has become a powerful tool for trade and commerce.William Gibson once famously said, "the future is already here – it's just not evenly distributed". What we can make of this statement is that this statement is very relevant to today's global trade and e-commerce. Digitalisation of trade has become a state policy in many countries. This is being done in order to simplify and interconnect all forms of trade that happens. The digital revolution[1] is transforming the way people interact with one other, with employers and employees, and with customers as technology is ingrained in nearly every aspect of our lives, from online shopping to job searching. Through digitalisation, business owners and regular individuals may connect with people worldwide, grow their professional network, and produce an increasing number of helpful and high-quality products and services. Since digitalisation of trade helps in bringing people closer to each both at the micro and the macro levels of the economy we can say that digitalisation has been a net positive especially for developing countries like India where digitalisation drives like Digital India helped in increasing the Internet penetration rate from 14% in 2014 to more than 50% currently. Digitalisation and internet penetration has helped in facilitating financial inclusion like giving bank accounts to those who did not have access prior to the digitization drive and digital payment platforms like UPI and BHIM have helped in making transactions easier thus bringing in more people to the economic fold. Digitalisation drives also facilitate employment opportunities for millions thus increasing employment rates and becoming crucial for the economic growth of the country. However there are many issues that are going to arise as a result of further digitalisation. As William Gibson[2] in his work

[1] https://www.niti.gov.in/sites/default/files/2021-09/The-Role-of-Digital-Infrastructure-in-socio-economic-development-042021.pdf

[2] The person who coined the term cyberspace

"Neuromancer" had specifically stated that cyberspace is vulnerable. So with more digitalisation comes more challenges that must be confronted.

Chapter - II

Research Questions

1. How is Indian cyberspace vulnerable?
2. Why digitalization in inevitable?
3. What makes GDPR the best cybersecurity legislation in the world
4. How can be done to improve Indian laws with respect to cybersecurity and why it is necessary in the current era

Vulnerability of Indian Cyberspace

India faces sophisticated and persistent cyber threats from state-sponsored and non-state actors that target India's strategic, economic, and national interests. This is due to India's outdated or inadequate cyber security policies[3], infrastructure, and awareness, which make it easy for hackers to exploit the gaps and weaknesses in the system. The event in which the servers of Air India were compromised serves as a suitable illustration of this type of data breach. Air India, the national airline of India, was the victim of a serious cyberattack. In this event, credit card numbers and passport numbers belonging to passengers were also stolen. This cyberattack can potentially have an impact on other international carriers. The data from August 26, 2011, to February 3, 2021, has allegedly been altered, according to the news agency ANI. Included are your name, birthdate, phone number, passport details, ticket information, and credit card information. Because of this attack, the personal information of about 45 lakh people was made public. These days, data is just as important as money. India has a vast population, thus many multinational firms are trying to get into the country (like Google and Amazon). This means that issues like internet governance, data localisation, and data sovereignty need to be addressed. By 2024, the digital economy is expected to contribute 20 percent of India's GDP, up from its present 14–15% share.Thus, issues like internet governance, data localisation, and data sovereignty need to be addressed.

Evolution of data privacy laws

The very concept of data privacy has come into the picture very recently during the course of history. Data privacy is one of the few topics that has changed so quickly in terms of public knowledge and understanding. Transborder data flows required restrictions in the 1980s due to increased globalization and the growing likelihood of data crossing international borders. As a response, the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were developed by the Organisation for Economic Cooperation and Development, or OECD. The OECD[4], which has a large number of member nations, seeks to reconcile the many interpretations of privacy principles that are upheld in various legal systems. The fundamental privacy concepts listed below were developed at that time and have been evolving in response to new requirements. Though the idea is not new, the last 20 years have seen a dramatic increase in the acquisition of personal data, which has fundamentally changed how the public, businesses, and governments see privacy. Because social media and other contemporary business models heavily rely on the flow and analysis of personal data, users of ad-funded goods may utilize them without fully understanding the nature of the transaction. Businesses of all stripes are becoming more conscious

[3] Is India's Cybersecurity system and outdated system on life support(Vol 7, No 3), International Journal of Mechanical Engineering

[4] https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

of the risks associated with managing sensitive customer data irresponsibly as a result of the rising frequency of data breaches and privacy enforcement actions. Early on in the development of the internet, "security" took precedence over the idea of "privacy." Early internet users became accustomed to email and password memory, so businesses had to come up with new strategies to stop fraud and data theft. For the typical user, security and privacy were synonymous; data usage beyond its intended use, let alone sale to advertising, was still unheard of. However it was only in 2017, the issue of data privacy ended up being one of the concerns for all internet users. This was after one of the greatest data breaches known as the Equifax data breach.[5]

In the Equifax data breach of 2017, the failure caused by the vulnerability in the intrusion detection software mechanism of the portal led to a loss of almost $ 1.7 billion. This was a major incident in the history of intrusions and privacy invasions caused by hackers in cyberspace. This was predicted long back by William Gibson in his works. This underscored several financial implications of an unsafe cyberspace and the impacts it would have on both, internet users and investors.

This incident was a reminder that there was a need for tougher laws for data breaches.

The General Data Protection Regulation 2018 also known as GDPR[6] has been the benchmark for all cyber data protection laws across the world. The law traces its origins to the year 1995 when the European Data Protection Directive (Directive 95/46/EC) was adopted by the European Union. From 2011 onwards there began a series of updates to the legislation that brought in a lot of changes especially when there were massive developments in cyberspace and technology with improved Digital Infrastructure and increased internet access. In 2015, European Data Protection Supervisor made his recommendations known to the European co-legislators involved in the GDPR's final draughting. He also introduces a smartphone app that contrasts the newest texts from the Council and Parliament with the Commission's plan. After the Equifax data breach, legislators in the EU stressed on the importance of data privacy laws and sped up with the implementation of the GDPR. In 2018 it was finally enacted and applied to all European Union member states.

The one other legislation that is known for data privacy is The California Consumer Privacy Act[7] which was implemented in 2018. The CCPA was created by Rick and Alistar Mactaggart, who were inspired to take action after Rick experienced identity theft. An essential part of the implementation is the law making process in California. California has ballot initiatives. It allows citizens of California to enact laws without the backing of the governor or legislature. A proposed law is put on the ballot if it gathers enough signatures, and it becomes a law if it receives 50% plus 1% of the vote. People get an exclusive front row seat to the creation and enactment of laws. The CCPA defines “personal information” as information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

In India the development of data privacy laws can be traced to one landmark judgment. The ruling in Justice K.S. Puttaswamy (Retd.) & Ors. v. Union of India[8] by the Supreme Court hastened the development of data protection and privacy regulations in India. Justice K.S. Puttaswamy (Retd.) and

[5] https://sevenpillarsinstitute.org/case-study-equifax-data-breach/

[6] https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[7] https://pro.bloomberglaw.com/insights/privacy/california-consumer-privacy-laws/#:~:text=The%20California%20Consumer%20Privacy%20Act%20(CCPA)%2C%20signed%20into%20law,1%2C%202020

[8] AIR 2018 SC (SUPP) 1841, 2019 (1) SCC 1, (2018) 12 SCALE 1, (2018) 4 CURCC 1, (2018) 255 DLT 1, 2018 (4) KCCR SN 331 (SC), AIRONLINE 2018 SC 237

others initially brought this case in 2012, arguing that a citizen's right to privacy was violated by the Indian government's proposed biometric-based identity card scheme for accessing governmental benefits and services. With this ruling, the Supreme Court established a standard for determining whether a government action would infringe upon the right to privacy as guaranteed by Article 21 of the Indian Constitution.

The present statutory foundation for India's data protection and privacy regulation is the Information Technology Act of 2000 (IT Act), which was passed in the previously mentioned context. Adopting the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 was one such modification. While the regulations offer some protection for personal data, most of the regulations concentrate on offering recommendations for improved security of sensitive personal data, which is a more limited category of personal data.

The Information Technology Act (IT Act) of 2000[9] includes several provisions for data privacy[10]

Section 43A- Requires organizations that handle sensitive personal data to maintain reasonable security practices and procedures. If they are negligent, they are liable to pay compensation to the affected person.

Section 72A- Provides punishment for intentionally or knowingly disclosing personal information without the consent of the person concerned. The punishment can include a fine of up to Rs. 5,00,000 or imprisonment for up to three years.

Section 66F- States that cyber terrorism is an act that threatens India's sovereignty or the public. Knowingly using a computer or system to commit acts of terror can lead to up to life in prison.

These are the 3 important provisions in the Information Technology Act 2000 that deal with data privacy and cybersecurity. It wasn't until recently that lawmakers started taking the issue of data privacy and cybersecurity seriously. This was due to various threats posed by hostile actors who consider the Indian Republic to be an official enemy. The first step towards this was the introduction of the Personal Data Protection Bill 2019.

This was one of India's first steps towards data privacy and cybersecurity both from a technological and a legal perspective.A Committee consisting of elected Members of Parliament[11] from both the government and the opposition was formed to evaluate and assess the provisions with respect to the statute. The committee recommended a lot of changes to the legislation which resulted in the new law titled Digital Personal Data Protection Bill 2022 being drafted. The Digital Personal Data Protection Bill, 2022 aims to establish a framework for organizational and technical data processing measures, establish standards for social media intermediaries, facilitate cross-border data transfers, hold entities processing personal data accountable, provide remedies for unauthorized and harmful processing, and establish a Data Protection Authority of India for the aforementioned purposes. It came into force from July 2024 onwards.

Analysis of Legal Provisions

The GDPR has a reputation for being one of the most robust data protection regulations globally. Although its main goal is to safeguard personal information, it also includes a number of important regulations that improve cybersecurity measures. The GDPR includes key elements that help to make it a powerful law for cybersecurity. The implementation of the Digital Personal Data Protection Act (DPDPA) 2024 in India marks a major advancement in safeguarding data privacy and protection within the nation. Nevertheless,

[9] Post Amendment in 2009

[10] https://www.scconline.com/blog/post/2020/02/06/evolution-of-data-privacy/#:~:text=Privacy%20was%20statutorily%20recognised%20globally,provisions%20in%20their%20domestic%20laws

[11] A committee headed by the Minister of Information Technology https://prsindia.org/parliamentary-committees/joint-committee-on-the-personal-data-protection-bill-2019

the DPDPA falls short in various aspects when measured against other worldwide data protection regulations like the GDPR in the EU.

While the GDPR applies to both personal and non-personal data in specific situations, such as data that has been anonymized but can still be linked back to an individual, the DPDPA 2024 specifically focuses on digital personal data. It does not include the safeguarding of non-personal or anonymized data, which can still be used for re-identification, reducing its scope. The main focus of the DPDPA is on personal data that has been digitally processed. This excludes unregulated offline personal data processing, causing a gap in the broader data protection framework. As per Article 33 of the GDPR, controllers are required to inform the supervisory authority within 72 hours of discovering a data breach, unless it is unlikely to pose a risk to individuals' rights and freedoms. According to Article 34, in cases where the violation presents a significant threat to individuals, they should be notified promptly as well. This guarantees openness and responsibility in managing cybersecurity breaches. According to Article 5 organizations must not only adhere to GDPR regulations but also show that they are in compliance. This clause mandates companies to keep records, perform DPIA[12]s, and designate DPOs[13] in specific situations, fostering a culture of accountability and openness in data protection.

The most important provisions in the GDPR which make it the best cybersecurity legislation are

Article 20- Right to data portability; This clause enables people to obtain their own information in a format that is organized, widely used, and can be read by machines, as well as to move it to a different controller. This lessens the dangers related to too much data processing and enables secure and efficient data transfer methods.

Article 30- Records of processing activities; Organizations are required to maintain comprehensive records of every data processing activity. This allows for improved surveillance of data security and possible weaknesses in processing systems, which helps to avoid breaches and unauthorized entry.

These are the main provisions in the GDPR that make what it is meant or is known for across the world, the most advanced cybersecurity legislation. Many countries look up to it as the source for their own laws. On the other hand the DPDPA lacks certain provisions that prevent the easy transfer of data and rules with respect to which server locations transfer of a consumer's personal data can happen at the will of the companies. The GDPR has strict laws and even harsher penalties for companies that refuse to comply with the same.[14]

Impact of cybersecurity in Global Markets

The main question of this research is how global markets and trade are going to be impacted. The answer to this lies in one simple issue which is the issue of data privacy. Investors generally pull away from companies that have a history of weak data protection regulations or have a history of illicit trading of consumer data without the consent of the user.

On an international scale, countries with weak cybersecurity laws and a weak cybersecurity are seen as vulnerable and investors and Information technology related companies prefer a limited or no investment and activity in such countries due to a heavy risk of breach of their servers and they end up realizing that cyberspace here is often unsafe and end up taking u-turns in their decisions and policy.[15]

[12] Data Protection Impact Assessment.
[13] Data Protection Officer
[14] https://irglobal.com/article/evolution-of-data-protection-law-in-india
[15] Dominique Shelton Leipzig(May 25, 2022), How attention to data privacy will stabilize our financial markets, World Economic Forum,

For a developing country like India, it is a must that we develop strong laws with regard to consumer data. Article 21 of the constitution empowers citizens with the right to privacy. Protecting a person's privacy in cyberspace is a Directive Principle of State Policy and should be one at least in the current age of the internet. Cyberspace is having a lot of power and as it is said "Data is the new oil" the government of India must step up and bring in tougher laws with regard to cybersecurity and protect the interests of the country.

Chapter - III
Conclusion

What we can understand from the research is that first cyberspace is complicated and requires a specific set of laws to govern it. No country in the world can escape from the process of digitalization because everything has to be computerized and in a country like India where the population is close to 1.4 Billion we can't have everything running on paper and that is not sustainable over the long term.

Second is that trade today is vastly digitalized to a massive extent. And digitalization of trade has brought that under cyberspace it has become even more important for the Indian government to implement tougher laws on any form of breach. The Air India hack of 2021[16] was a warning sign to all users and investors and other people involved in the Information Technology sector that their very day to day life is vulnerable and hackers have their eyes everywhere. The other main purpose for hackers having access to everything is poor data transfer and server related laws. In the EU where the GDPR is enforced the servers must be within the EU zone and must take instructions from the EU legislators and authorities. Although India is catching up there is still a lot to be done.

Chapter - IV
Policy considerations and future recommendations

Even global stock markets are impacted by the policies[17] that are there with respect to cybersecurity and will only continue to have a bigger impact further on. Weak cybersecurity laws often lead to hacks and manipulations which investors and agencies want to avoid, so they avoid countries where such laws are non existent or lack proper enforcement.

India needs improvement in the cybersecurity and digital data protection laws,[18] but is heading in the right direction at least with one at a time being implemented correctly. What we need is to reclaim sovereignty of our servers and this is not going to come without geopolitical pressure. Many geopolitical experts claim that cybersecurity legislations are either unenforced or weak in global south countries due to the fact that countries in the Global North add pressure. But in the case of India, the policy is being pursued in the right direction and it must be a role model for many in the global south.

India must go ahead with reforms and massive digitalization of Indian economy. Just like the concept of UPI was a massive success to which the entire world takes an inspiration from a data protection legislation can do the same as well.

[16] https://www.forbes.com/sites/carlypage/2021/05/23/air-india-data-breach-hackers-access-personal-details-of-45-million-customers/

[17] Joshua.P. Meltzer(May 2020), Cybersecurity, digital trade and data flows, Global Economy and Development, Working Paper-132

[18] Bhumesh Verma (Feb 6 2020), Evolution of Data Privacy, SCC Times, https://www.scconline.com/blog/post/2020/02/06/evolution-of-data-privacy/#:~:text=Privacy%20was%20statutorily%20recognised%20globally,provisions%20in%20their%20domestic%20laws

Chapter- V

References

1. Joshua.P. Meltzer(May 2020), Cybersecurity, digital trade and data flows, Global Economy and Development, Working Paper-132
2. Naman Agarwal, Mohit Rao and Himanshu Agarwal (March 2021), The role of digital infrastructure in socio economic development, Invention Intelligence
3. Paul Nyrén, Oscar Isaksson, The value of cybersecurity: Stock market reactions to security breach announcements
4. Joshua Kroeker(26 June 2024), Mind the digital gap Please!, TMI Innovation Lab, https://innovation.treasury-management.com/mind-the-digital-gap-please/
5. Ankitesh Kumar Kha, Aditi Kumari (3 March 2022), Is India's Cybersecurity system and outdated system on life support(Vol 7, No 3), International Journal of Mechanical Engineering
6. Olena Kravchenko, Maryna Leshchenko(2019), Digitisation as a global trend and a growth factor for a modern economy, SHS Web of Conferences 65, 07004
7. Robin Adruss(June 27, 2022), A brief history of data privacy and what lies ahead, Skyflow, https://www.skyflow.com/post/a-brief-history-of-data-privacy-and-what-lies-ahead
8. Bhumesh Verma (Feb 6 2020), Evolution of Data Privacy, SCC Times, https://www.scconline.com/blog/post/2020/02/06/evolution-of-data-privacy/#:~:text=Privacy%20was%20statutorily%20recognised%20globally,provisions%20in%20their%20domestic%20laws
9. Colleen McClain(Oct 18 2023), Views of data privacy risks,l personal data and digital privacy laws, Pew research, https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/
10. Dominique Shelton Leipzig(May 25, 2022), How attention to data privacy will stabilize our financial markets, World Economic Forum, https://www.weforum.org/agenda/2022/05/how-attention-to-data-privacy-will-stabilize-our-markets/
11. Samuel Mani (June 6 2023), Evolution of Data Protection Law in India, IR-Global, https://irglobal.com/article/evolution-of-data-protection-law-in-india/