IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

LAW RELATING TO DATA PROTECTION IN INTERNATIONAL TRADING SYSTEM

ARUSHI MEHRA

LLM (INTERNATIONAL TRADE AND ECONOMIC LAW)

Co-Author

Dr. SALTANAT SHERWANI

AMITY LAW SCHOOL, AMITY UNIVERSITY, NOIDA

ABSTRACT

In international trading system which mainly aims on goods and services which basically focuses on across the borders of countries. It focuses upon import and export of goods and services which is most important for economies of the countries. The foreign trade which provides countries to trade their goods and services beyond international borders system. The trade in global system which also mainly focuses upon three C's which are compliance, content, and connectivity on trade.

The data in the trade which mainly has the details of importers and exporters and information upon the product information. The trade which also involve and covers the data of importers, exporters, bankers and also of logistics who involve in trading of any product. The information which also collected by each country while trading.

Data protection which involves international data which flows the consequences for trade and also the development, according to UNCTAD which is most coherent and the likeminded data protection regimes which only be more important in the face which can incorporate new technologies such as cloud computing, big data and the Internet of Things.

Thus, this research has been undertaken to study the role of WTO, GATS and many more perspective safeguarding the data protection under international trading system.

KEY WORDS: Issues, Role of OECD, APEC, CPTPP, GATS.

CHAPTER 1

INTRODUCTION

Data localisation and data globalisation proponents have recently been at odds with one another. The former have been advocating for an open and unfettered movement of data across borders, whereas the latter have been taking actions to restrict this flow while raising privacy and security concerns. The storage and processing of data must take place on the soil of the nation implementing such regulations, and thus data localization policies broadly restrict or outright forbid cross-border data flow. Most studies indicate that these forced localization initiatives place a significant financial burden on firms, especially small and medium-sized ones (SMEs), by raising the price of procuring local computing resources and data storage infrastructure by 30 to 60%. Actually, according to a research by the European Centre for International Policy Economy, Infrastructure for local data storage and computing. According to a study by the European Centre for International Policy Economy, mandatory data localisation regulations have a significant detrimental impact on investments as well as the GDPR. However, nations that implement such laws defend the necessity for data privacy, cybersecurity, and defence against unauthorised foreign spying. There is some validity to these worries. Many more nations began implementing data localisation requirements, especially in the wake of Edward Snowden's revelations about the National Security Agency's massive surveillance programme.

The rule in the privacy and personal data citizen And residence on protected as fundamental right there by describing them the highest normative value. The European Union who has also adopted the General Data Protection Regulation, (GDPR) for the protection of the data which entered into force in 2018. This can be extended to include the transfer of personal data to any third countries only for regulations where is intended to guarantee a high level of protection of personal data and not be destroyed by finally, the law only applies to cross-border trade. Transactions involving certain personal data from the EU. Even is a type of organization that can operate outside the EU., then such kind of external effect which may also profoundly impact the suppliers who deal with goods and services from outside of the EU.

The funding potential of international trade law to conflict with sovereign parties. In order to protect the privacy in which the verdict was delivered from the 1994 General Agreement on Trade and Services (GATS) even as multilateral international trade agreement which concerning international trade in services. There are many kinds of authors who has compared European Union regulations on the transfer of personal data in the context of prosperity order against some of the provisions which involved in the GATS trade isolation disciplines.

Data Protection Role In International Trade

The increase usage of an internet and communication technologies usage which has bring a rising awareness in the protection of personal data which may require right to privacy of a person. Even in digital trade which has increased the data flow from one place to another throughout the internet. There are many various types of laws and agreements made for the protection of the personal sensitive data of a person in international trading system.

Even in global information economy, in which now a personal data which have become the most important existing online activity. Even every day, a vast amount of information which was transmitted, stored and also get acquired from all over the globe by a massive improvement in computing under power of communication. Most developing countries which are so much emerging in online surrounding, economically and also activities include financially which has been enabled through phone and connectivity from internet only.[1]Protection of a data online, which is the most significant challenge for anyone to safeguard. Security of information which is also a main concern for any government, businesses and also for consumers. Even in the international trade perspective the developing countries provided domestic legal protection with business opportunities as a possible result in international trade. But, still most of the developing countries still lack behind in securing in the protection of data and privacy in trade.

The most large amount expanse of an information and its necessity upon which have expansional increased, but in other way government also assert by controlling the data globally which also has some of flows and change much drastically by applying influence upon matters which are happening out of the way of borders which was illustrated by French judgement under the yahoo case.[2]It can be said as Internet censorship which may pause as practice by the China and many other countries which are well known example of controlling of data. But still the new group of people through net control keep to seeking of information from went out of a country rather than pausing it from entering in the sovereign spaces of the State. Even though the government localized the usage of data information regarding their jurisdiction for a various kind of issues, but also to ensure this kind of erecting barriers to data information flowing which may become as a barrier upon trade, which may dangerously affect the realisation of data economically innovation side by side. This kind of provision of any digital production and kind of facilities comes in cloud computing applications or we think in future most of future oriented terms or the kind of apps which may be used the (internet of things) IoT or artificially intelligences which may not work according to the limitations on the crossing flowing of data from borders. The territories where most of the data protection also comes with a certain kind of costs for the countries, by adopting such kind of majors, to protect themselves from the cyber threats to protect their data while in trading through international system. It also includes global data flows which also has changed over all.

1.1 How data protection in international trading system

The kind of information which always has been a most important and most subtle unique for some of the company, states and also for citizens as well. This mainly join one data with another by flowing some of the information on data by crossing through the territories and by protection which needs national interest, which is not entirely new, but for which concerned steps were taken.[3] But around in particular year, late 1970s and in 1980s in which most

[1] https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

[2] *The* LICRA *v*. *Yahoo* RG 05308 Year 2000

[3] C. Kuner 'Regulation of transborder data flows under protection of data and privacy law- Past, Present and Future', OECD Digital Economy, 187 (2011)

of satellites, computers and even the software's, which was not much deeply evolving the communication in which trade happening between the nations by granting the data flowing through boarders freely and also by some national laws which came as the most apparent approaches.[4] Even in each kind of concerns of a larger multinational company with which involve nations are concern about certain restrictions to information which flowing which may create issue or might affect economic activities and also looked for solutions that may resolve the problems of such kind of barriers which are affecting the data. Even born binding solutions which were found in the auspicious that the Organization for Economic Cooperation and Development (OECD) in apart of a principle which can sort to balancing of the flowing of data much freely with the nationally interest in field of private of information and even in the securing of a data.[5]

Even the OECD which means Organization for Economic Cooperation and development, in which in itself points out the kind of privacy framework pitch which underwent the kind of a situation then, which profoundly been different from challenges in realm of data of a governance we has been facing in today's scenario. In current scenario, the digitalization and the societal embeddedness of a digital media which has changed the volume of the surrounding and intensely of data flow[6]

1.2 The importance of data protection in international trading system

The data need protection which is most directly related to the trade in goods and services in the digital economy world. But insufficiently this kind of protection which may create a negative market effect by dipping the consumer confidence and also by overly severe kind of protection which can also overly restrict businesses and can affects in adverse economic as a kind of result. Even the emerging laws which considered as the world nature and scoping of their submission and emerging the temporary capability with other agendas is to be utmost importance of global trade, which follows higher increase much delight rely or depend upon net onwards. Even many kinds of social and cultural kind of notes which around the world include a respect for a privacy but which may also underlying some kind of privacy kind of principles which may contain many commonalities across countries, interpretations and applications in a specific duration which also prefer significantly from each other.

Some information regarding economy which is one of the most important which promises to provide many kinds of opportunities. But which also evolve certain kind of potential problems. Even internationally compatible of the

4 S. A. Aaronson, 'Why Trade Agreements Are Not Setting Information Free: The lost history and debate over cross-border data flows, human rights and national security' World Trade Review vol 14(2015) page-672, 680–685.

[5]OECD, 'privacy framework of supplementary of explanatory memorandum' Revised OECD privacy guidelines Paris: OECD, 2013.

[6] J. E. Cohen, 'What Privacy Is For', Harvard Law Review 126 of 2013, P-120-123.

data security regulations are desirable way to create an environment that is more predictable for every kind of stakeholders involved in informational economy and also to build trust under it.[7]

Even the value of data with some of risk which has associated with data connection, data processing, the data use and also the reuse of the data types with kind of companies and the governments which has dramatically changed over the years. But beyond the imperfect mantra of data being the new oil[8] or can be crude oil for which many countries with many kind of studies which also has point vast potential of data which has also triggered for more efficiently business operations, highly innovative solutions and kind of fed up policy choices in all kind of areas of societal life to be involved.[9] Over the horizon such kind of evolution of potentiality can refer not only to digital surrounding areas, such as searching of networking, or the social to bringing out mortal or on store business, like a production logistics. Wholistically, the result of big data readiness and analysis are multiple and some of which are far from reach and much beyond.[10]

Even in recent inquiries it is shown that only share sheer quantity of information and also our reliance upon the data which has exponentially risen on the contrary it also has given the options to the government to assert control over global data, which flows which also have changed so much.[11] By applying such kind of jurisdiction over online matters which are beyond borders exemplified by some kind of seminal French judgement in Yahoo case[12] or can also be called as internet censorship as a practice by the China and many other state which are best known examples for controlling a system.[13] The new types of Internet controls, which may search for only to keep information from going out of the countries, somewhat than by bring to an end it from getting into independent space. The government, who incrementally localized the information within the decision for a number of explanations.[14] By ascertaining, this kind of enacting kind of obstacles to information flows affects directly on

[7]Mr. Joakim Reiter, Deputy Secretary General of UNCTAD, 'Data protection regulation and international data flows: implications for trade and development' 19 April 2016. www.unctad.com

[8] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[9] Manyika, Mayer-Schönberger and Cukier, N. Henke .'The Age of Analytics competing in the data exclusion in the worlds' McKinsey Global Institute, 2016 Washington DC

[10] R. Deibert., 'Access Contested: Security, Identity, and Resistance Asian Cyberspace' (Cambridge, MA: MIT Press, 2011) Page-11-20

[11]Klaus Mathis, Avishalom Tor, 'New Developments in Competition Behavioural Law and Economics' Berlin Springer, 2019 Page- 241–263.

[12]Supra 2

[13] Irving A. Williams, Daniel R. Pearson, Shara L Aranoff United States International Trade Commission, 'Digital Trade in the US and Global Economies', Part 1,Page- 332-340(Washington, DC: USITC, 2013).

[14] Anupam Chander and Uyen P. L'e, 'Data Nationalism', Emory Law Journal Vol.64 Issue.3 (2015), 677–739 www.emory.edu.com.

trade on which may affect the overall information flow in an economy onwards. These kind of provision of any virtually available products and kind of offerings like computing over cloud applications or thinking in more future relying terms the (IoT) which is Internet of things and (AI) which means artificial intelligence that wouldn't only work under the restrictions on the borderless flow of information.[15] But inclusively, the data protectionism, which may also come at a certain kind of cost for the countries by adopting such kind of measures to protect the data.[16]

Finally, at the same time, a higher level of data protection often creates a problems for businesses where it is need to protect the fundamental rights of the public, the public interest and the public interest does not exist. However, much of the data collection you use and the implications of privacy protection have been acknowledged by many experts and many policy makers in recent years, and have been heard from casual users of products and services alike.[17] The certain types of risk which may also have been increased in the recent era of a big data, which has presents a certain kind of distinct tasks or problems for the protection of Personal data and ongoing protection of personal and family life issues. The difference between personal and non-personal personal information is the large amount of data that raises the question for the security of personal information of traders like importers or exporters.[18] The difference between personal and non-personal personal information is the large amount of data that raises the question. But on the other hand, may seem like one of the main tools for data protection, which means anonymization, means the process of removing symbols from creating a kind of anonymous dataset limited to data-driven values. but, it is true that will now be completely and irreversibly the

data generated by all kinds of user games.[19]Finally, on the other hand, big data also allows verification of the accuracy of the data examined by the use and combination of data and is non-personal, especially since information is not always available and non-personal. may include dedicated technology. forever. Big Data ensures that the elixir is incorporated into the core of existing privacy law, which also operates under the principles

[15] Article 7 Charter of Fundamental Rights of the European Union (CFREU) which distinguishes between the right of respect for private and family life and right to protect personal data under Article 8. https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

[16] M. Burri and R. Schär, Journal of Information Policy 6 (2016), 479-511.Journal of Information policy by M.Burri and R.Sachr2016

[17] Journal of Information policy by M.Burri and R.Sachr2016

[18] U. Gasser, 'Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy', Harvard Law Review Volume 130 Issue 2 December2016, Page 61–70. https://harvardlawreview.org/

[19]CJ Bennett and also RM Bayley 'Privacy protection in the era of the big data' Cambridge University Press https://www.cambridge.org/core/books/big-data-and-global-trade-law/global-trade-law-and-policy-in-the-age-of-big-data

of transparency and quality of users visibility. [20] Justice reveals that is another important concept of privacy protection, and as the most common companies, is famous for retaining a large number of different types of users. An example of is EU General Data Protection Regulation (GDPR). The conflict between most initiatives and the cultural and social context of law, public relations, and deep understanding of the role of government and business. Significant differences between and national privacy laws, specifically the EU's United States, the European Union and most trades are not affected companies and agreements which have become the worst of the shared standards for protecting this information.[21]Against the background of the complex and controversial environment special purpose information and cross-border information is a new topic in international trade negotiations.

1.3 Statement of Problem:

Statement of problem under data protection in international trading system is that the traditional argument which focuses on the leap of data privacy rules across the group and the lack of into possibility between these kinds of roles. Even in a connected world, some of irregularities which may raise a complex conscience over the transnational protection of privacies. The other problem is the lack of uniformity which may lead to additional complaints cause for companies and which may also limit the economic benefit of cross border data flows which happened between the countries. The other problem by adaptation rules and the GDPR. It does not allow the influence of cross-border e-commerce on some customers because it usually allows the transfer of personal data. The only thing that matters to the success of a business deal is the one thing to watch out for data transferring of any trader or of personal information transferring.

1.4 Objective and scope of research:

Main objective of my research is to provide information various type laws and type of agreements and new agreements which are in process comes and how to protect data. The laws we need is for the lack of data privacy, which may lead to misuse of personal data and result in costs for businesses and individuals, identity theft may not only cost users billions of dollars, but it may also cause non-economic costs, ranging from physical and emotional harm to negative effects on hardship and life opportunities of a consumer. Even though companies may expect consumers to provide their personal data, some consumers may end up paying higher prices, buying goods and services of inferior quality, and incurring transaction costs spontaneous communications for which these kinds of businesses may also suffer losses in online retail consumers price which may concern some negative publicity, administrative fines upon sanctions and massive class action by claims also. International trade agreement concerning international trade in services. European Union rules on cost, water transfer, and personal data are against provision of the GATS, which treats liberalisation disciplines that have found inconsistencies between the two.

[20]*Ibid*

[21] Jennifer Daskal, 'Privacy and security Across Borders' Volume 128, Yale Law Journal, 2018-2019. https://www.yalelawjournal.org/forum/privacy-and-security-across-borders

In particular, GATS involve of Article XIV which defines the scope of World Trade Organization (WTO) autonomy to regulate in the interest of privacy, which can be difficult to This has led to satisfy such kind of challenges legal for regulated previously GATS with the addition of trade liberalisation. The digital Agenda mainly focuses on taking trade liberalisation commitments further under GATS. The main objective is to provide type of agreements which are made for protection of data in trade.

1.5 Limitations of research

In international trade law which was previously totally disconnected from internet governance because of changes in legal and institutional structures. International trade law whose main concept to maintain the relationship among the countries in which internet which now to be considered as most important to be look upon. The main role WTO, GATS and also of EU GDPR in protecting the data of traders or can be said of stakeholder who work through globally digitally on e commerce way.

1.6 Research Questions/working hypothesis

For the purposes of this study, the hypotheses formulated by the author are as follows:

The increasing use of communication technologies which has mainly brought the awareness of in data protection and right to privacy. The connection to digital trade, global data flows which has assume a important by becoming the object of numinous international agreements, and also by requiring a further protection of personnel data.

1.Main issues which are arising in the protecting the data while in international trade

2.Acquiring of an international jurisdiction law making for amendable right to privacy and protecting of personal data in conflict of laws and to regulate fair and equitable trade.

3.Type of agreements which are made to protect the data in international trade.

4.What is the role Global Data Protection Regulation means GDPR for data protection.

5.Role of WTO, GATS in data protection in international trade and in cross borders.

1.7 Research Methodology

Research methodology which is most significant part of any research that will be adopted and followed for the purposes of this dissertation shall be Doctrinal. It will begin by laying down the building blocks comprising and leading up to the current law on protecting of privacy and also the personal data by searching through journals, books, articles and case laws which help in briefing the concept in much more vast ways.

18 Conclusions

There are many national laws which demand storage and processing of personal data locally on the Client Side. Protecting of the personal information of the traders to be protected which is most concern issues in recent legal scenarios.

CHAPTER 2

INTERNATIONAL TRADE AND FLOW OF DATA

International laws regarding digital production allow individual companies to control the sources of the guidance on data protection for customers. This should include two documents in which companies can participate in protecting information, such as EU and US procedures in which all can be set as Privacy Shield the APEC Cross border rules for privacy system which involve CBPR[22] (Cross-Border Privacy Rules System) or a great range of schemes for privacy and scope of their membership to a particular activity onwards. The wide range which is also classically published on registration of a non-line of U.S. Department of Commerce, list of Safe Harbour members OF APEC, CBPR directory of a compliance system for a various scope of restrictions. Even the limitation district coverage to online or offline kind of data collection, but the consumer or an employee. Data or any other broadcasting series. Even the Limitation may exclude the entire country from the protection which offered by the large multinational for example APEC and CBPR. The second one is that the company may exclude certain kind of activities from protection buying clouding a fine print exclusion in its public privacy policies. But this may increasingly some common organization to exclude certain kind of definite kind of services like mobile apps, cloud services, and software form the protection of data which also guarantees that may put on more largely to the businesses. This may help in exclusions which may often extended to a resolution of disputes where the company may also uses a 3rd party dispute resolution provider for resolving the issue. So, most of the exclusions can be quite important for the consumers.

2.1 INTERNATIONAL TRADE AND FLOWING OF DATA FREELY ACROSS THE BORDERS

Increasing business access to goods and services that can be provided over the Internet due to laws and regulatory issues requires to address some of the limitations of cross-border information for most important purposes such as protecting information between individuals and countries Security requires governments to restrict certain flows of information across borders may require. Market policy balance i.e. to ensure access to goods and services versus the government's need to restrict jobs to carry out more non-commercial activities. The WTO who has directed this issue which may make available some guidance. Even the government have already begun to identify the need to find different ways to manage these at the time of compering the policies goals. But for some, OECD also made some points in its Committee Consensus on Internet Policy Development Principles. The information should now be free. Other prisons completed within the framework of promote freedom of information, noting that is also an important part of the government's commitment to improvement personal information is protected by cybersecurity solutions. In 2011,KORUS became the first international agreement to have mandatory rules for the cross-border transfer of documents. Such actions are advisory only, as most parties should try to avoid crossing the border or manage problems that do not harm the electronic data flow. Also, this interpretation of this contract

[22] APEC, Cross-Border privacy Rules System'
https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules system

differs from the parties' right to accept the restrictions on the Internet based on the statutory exception to the contract.[23]

2.1.1 National Security

The Internet which has become increasingly surrounded the economic life, countries which are at a growing risk by the cyber attackers whether by an individual or by criminal networks organizations or even by government also. Even former defence secretary whose name is Panetta who has also detected that the internet which is open which need to be highly manageable because of its need. It has also provided a new form of fear for conflict concerned and battel field for the future concern as well.[24] Even in 2012 in which Saudi Arabian State Oil Company Aramco who got attacked. The company which got hampered and demolished over 30,000 computers, which was emphasized the threats, which was stood by the cyber security to the nation's structure critically in a large way. The act to address these kinds of threats which may only need by protecting serious networks by recognizing and by addressing certain kind of possible cyber threats. Even cyber threat, is a concern which could affect on the readiness of the countries to grant certain kind of flows on information crossways borders.

2.1.2 Personal electronic data

By ensuring the adequate protection of personal electronic data across borders which is a wide concern for government which has consequences for the ability to transmit or to send any kind of information across borders by government. One of the main issues is that the countries take various methods for protecting their privacies and to exporting data of consumers. But some example, like Australia which permit data to be carry across to jurisdictions with some of substantial same levels of privacy of data protection.[25] Even in the US, the FTC has established privacy guidelines under Government action to protect their data, with companies collecting and using information they want to comply with, and working with companies that don't. .[26]But European Union EU whose Data protection avoid the export of data to other countries who has any lesser privacy data laws provided by countries.[27] EU which also got introduced only to discourse or tell about different kind level protection of data by EU. But EU which also applied only to transferring of personal data to any other third countries in the process.

---

[23] Joshua Paul Melttzer 'The internet, cross border data flows and international trade' Asia & Pacific Policy Studies, Vol 2 Issue1 page 90-102. https://onlinelibrary.wiley.com/doi/full/10.1002/app5.60

[24]Ibid

[25] https://www.ag.gov.au/about-us/careers/statutory-appointments/privacy-commissioner#:~:text=The%20Privacy%20Commissioner%20is%20responsible,certain%20private%20sector%20organisations%3B%20investigating r

[26] FTCR REPORT 2012 on protecting privacy of a consumer available https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

[27]European Parliament and council on free movement of data 24 October 1995

[28]The law regulates different levels of data protection in the European Union and also the transfer of personal data to other countries.[29]

Private law and its impact on international trade. Currently the IEA also has now being provided under the international bodies of economic as well in 2005, Asia Pacific Economic Cooperation APEC adopted the APEC Privacy Framing, which includes nine sets of principles that provide guidance for the advancement of private rights in the APEC economy. The privacy framework for APEC can find secure data security in by protecting private data without interfering with cross-border transmission of information. Section is concerned with whether cross-border information transfer will be from individuals' ability to receive only through their ability to protect information, not their ability for country.[30]The government may also have access to personal information as part of an investigation in criminal or for any other national securities reasons which comes in another problem which may Affect the peoples willingness to make available data online that may be essential for transactions happened commercially and even for international trade to happen. Government is also the one who exists such kind of data, which is neglected differently across the countries globally.

2.1.3 Political Parties

The Internet, which has now become the big challenge for political power in large ways. Even for example, the famous uprisings which include Tunisia, Burma, Iran, Egypt and in Ukraine the countries who were simplified by the interconnectivity made by possible by the network in the large manner.[31] The Internet reporting which has motivated the Internet restrictions, which involve blocking access to the media reporting on the complex and also sensitive political issues which are using the Internet as a site to express certain kind of their views point, which may also considered as harmful for the government in many ways. Such kind of restriction can also be used in name of security for nationality, but by highlighting such certain kind of scope security for nationality only to defend a wide-ranging of restrictions on internet which are to be mandated.

2.1.4 Commercial Restrictions

Restrictions, which happen in information flows can also be commercial in nature. Such kind of resolution, which diminish the ability of buyers and also the sellers for transactions and the companies who operate across crossways borders also. In the end, these problems were mostly decided by the success of foreign companies and to repeat their success by the government using digital form of child trafficking laws to protect internet businesses from foreign competition. These internet trade restrictions may affect the domestic traffic of

[28]Article 25 on personal data and also free movement of trade

[29]https://elibrary.worldbank.org/doi/abs/10.1596/0-8213-5408-6 Article on domestic regulation and liberalization in WTO.

[30] Martin Abrams, 'The Strategic Front: Why Should We Care About APEC Implementation Privacy and Data Security' APEC L.JPage: 22-34

[31] Bruce Etling, Robert Faris and John Palfrey, 'Political Change in the Digital Age: The Fragility of Online Organizing Summer-Fall 2010 ' SAIS Review Vol. 30 no 2 Page-43-49

domestic companies, but they are sufficient to block retain sites or access to the internet so that users can navigate to other websites, including national websites..

These decisions on the Internet are often detailed, but is not easy to understand and is not expressed in an arbitrary or incomprehensible way. For example, a foreign company, may not know about it and the website may be banned if it is visited a lot. Foreign ISPs are also often unaware that the government uses created designs to block certain websites. This, will also create a risk that a particular kind of website or Internet service that are available for one day but may not be accessible for the next day which makes it hard to run an online business which makes slow accesses to a certain sites which may deter consumers by leading them to use other online business domestically basis. These kinds of restriction which may also affect sales negatively, even revenues to advertise and also to scopes and dimensions of international trade side by side.

The government may also gradually by demanding businesses to locate them in data amenities within their territories only. But in much of such cases this raises the costs of providing of the certain services that get rely on data flows such as cloud computing involved in it. In addition, the government has access to local data storage, This, can reduce the need for consumers and businesses to share some personal information and use cloud services, which can sometimes lead to information. services providers to make their leaving from the market and departure from domestic businesses with certain kind of access to make it much less effectual and also fewer effective services which can reduce their main ability to complete domestically and also in overseas market to access data. [32]

2.2 SUGGESTIONS OR STEPS TO BE FOCUSED ON WHILE TRADING

❖ The Development of necessary commitments with omissions: the sufficient regulations must begin to ensure that cross-border data flow is legally required while giving governments adequate space who may restrict the flowing of data which may necessary to achieve the other legitimate policy goals. This kind of limitations should also be get designed and must be get applied in a certain non-discriminatory and smallest amount trade restrictiveness and also in the visible manner onwards.

❖ The flow of data in intra country: The commitments which on cross border flowing of data which may involve a promise which should not limit intra countries flowing of data. There is no presence of commercially any kind of reasons for certain rules on cross border flowing of data by not applying to their movement within the country and even once a data is allowed across borders with many of the explanations for a government restriction on any of intra country data which flows reduce but not entirely get disappeared.

❖ Standards which come internationally: The global standards industry and also interoperability criteria which will underpin the growth in cross border data gets flow which include the ability of the users to access and also

[32]M. Burri, 'The International Economic Law Framework for Digital Trade', UNCTAD Volume 135 Page: 10–72

use of digital content across the devices onwards. Even government should also pledge to the developing of standards internationally with the main objective of underneath the developing of technology that is much reliable with source internet operations.

❖ Centres use for data locating: the centre of data which is located domestically and may challenges the most cost efficiency which is stored on cloud created by computer services which were located and its independence is much more important. But underneath the KORUS whose members may have organizations for flowing or transferring of crossing the data through borders for data processing regulations.[33] The governments who should also commit to similar kind of instructions for all kind of computer based only upon singularly on computing services onwards.

❖ Transparency instructions: Internet which has certain limitations on across border flowing of data which most often may get applied on an arbitrariness and upon non transparent method. But some of FTAs which have kind of regulations which may require much transparency and also due process which has yet more norms needed. There is much more internet limitations on cross border flowing of data which may raise a specific kind of problems that may require additional promises in following areas as follows:

- A contract which has selected point in the government agencies who are accountable for certain kind of limitations on across border flowing of information.
- A certain kind of provision on progressive notice of any kind of proposed actions which are affecting across border flowing of data which may include the certain kind of issues for the proposed limitations.
- There are certain chances for parties who are interested which involve businesses or an individual who may present their own viewpoints upon the proposed restrictions and also a need for requirement for written and on the rational responses as well.
- There are also certain opportunities for administrative review of data flow restrictions.

❖ Norms which get develop while cross- border data flows: Even the governments may also prioritise or make important developing standards which happened among the governments with some of respect to flowing of data. By addition to the part of necessary trade rules where government should make certain kind of principles for governing the accessibility for using of the data.

❖ Digital drive addressing: The businesses, which happening under developing countries whose non-tariff cost with such as inadequate logistics and also services for transportations which has a significant effect on the cost of exporting as well. It is also noted that growing usage of Internet accessibility in the developing countries, which

[33] KORUS Annex 13-B, Section B available https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

may reduce the cost of exportation by up to 65% under it.But by supporting developing countries with much betterment by take part into trading system happening globally which increasingly in large.

CHAPTER-3

INTERNATIONAL INITIATIVES ON DATA PROTECTION IN TRADE

International initiatives taken internationally or globally for protecting and safeguarding for data of traders like exporters and importers who comes together for trading.

3.1 WTO

The World Trade Organization (WTO) is an undeniably important part of
organizations. On the other hand, it is important in terms of protecting intellectual property rights numbered, which shows the rights to trade in goods and services numbered as a complex process. On the other hand, many times there are only more ways. Politically, however, the failure of many systems on some issues led to preference to take action on these issues, and this was particularly evident in the field of digital marketing, as later pointing out.

3.1.1 Development of WTO Agreements

This is the basis of international commercial law, ratified during Uruguay Round
between 1986 and 1994 and entered into force in 1995. ITA, amended in 2015), WTO rule remained unchanged and largely in its pre-Internet state. It can be argued that the law does not necessarily change in every new technologies. In fact, WTO law lends credibility to the argument because it is flexible in many ways, both in substance and procedural. Although there are, the World Trade Organization (WTO) has the potential to be creative and effective at home. It may be included in the regulation or penalties for breach of duty. It is also based on key discrimination principles, such as Most Favoured Nation (MFN) and National Treatment (NT), which cover all areas of economic life and possibly technological development. But there are many laws, including the structure, business principles, on the implementation regarding the standards on the facilitation of protection of data transferring.

3.2 Advantage of WTO

The strength of WTO law is that although it is law and focuses on trade rules, it also allows for some flexibility. One of the most important is the XX article of the Trade and Industry Agreement (GATT)will violate the agreement if discriminatory or unreasonable or those measures that impose trade restrictions between countries of similar content are implemented. . At the core of commerce is the negotiation of information flows, which have many possibilities under GATS section XIV that can manage existing information and use new ones. Section XIV

lists as many different terms as possible, including two specific terms related to: (a) areas of public order or public administration fairness, and (b) protection of privacy such as law or reasons required by law; or regarding the processing and disclosure of information and protecting the privacy of personal information and funds. According to the article, people argued that for example the provisions of the GDPR could be considered a violation of EU rules under the GATS.

The following section provides an overview of the development of PTA over the past two years as the digital marketing management space has grown. Document is derived from our own TAPED document (full in the Electronics and IT Industry Business Contracting Rules), which provides a detailed map of the subject and the coding of all PTAs including chapters, regulations, appendices or annexes. Documents that directly or indirectly regulate digital commerce. In the continuation of we will examine the new rules for free data and the structure of in multiple PTAs. It also examines in more detail the model of digital trade regulations that we currently have, namely the Agreement and Agreement on Cooperation for Cooperation (CTPPP) and some subsequently developments of in the United States-Mexico-Canada Agreement. (USMCA).4% includes world GDP of 13,5trillion, still the 3rd largest deal after NAFTA

and even the EU single market. Across the border, trade-related and most importantly CPTPP was established. E-Commerce also comes across as the best model to date in the landscape of the PTA. It has also has 18 articles,13(2) prohibits either party from using or giving the location of to barbarian any place deemed to be in the territory of the party, under conditions of doing business in that area. United States, South Korea donation agreements, information donation is now mandatory for all participants information should be allowed to cross the border electronically, for many activities there will be personal information. business from only insurers. 35 In this law, is general, most information transmitted over the internet will cover, but the word "to" can mean that it should be some kind of exposure pain. There are some restrictions on the digitized flow or localization of information

3.3 CPTPP (Comprehensive and Progressive Agreement for Trans-Pacific Parternship)

The data transmission is more than data needed to implement some logic. The same distinction as the tests specified in GATS Article XIV and GATT article 2XX is to equate, commercial and non-commercial grades. The term CPTPP test differs from WTO rules, especially when GATT has a public list of target rules, even when calling social protection or GATS as public order. However, the CPTPP can provide new clauses and may only be used for public policy purposes. This license, offers CPTPP signatories more autonomy. But, however, this can lead to all the legal uncertainty, but further reduction of restrictions regional measures for financial services and institutions should be noted. Financial Services Section states that we have specific decisions regarding the privacy of personal information, or perhaps CPTPP Art. 14.11(2) for attention to the state is working. Under Article 17 Members of the CPTPP shall not be sought to modify or transfer the terms of any software that may be owned by another person as a license to import, distribute, sell or use. Any software that can still be modified before is of any kind in its territory. Attention required only for large software businesses Products may contain custom software types. This also leads to the completion of software and custom products for infrastructure and commercial delivery contracts that will be important. The main purpose of this article is only to protect software company and address their concerns about IP slack or issues in their security procedures code onwards.

Even in Section 14.8 requires equipment to include all CPTPP members to recognize and maintain a legal framework that provides certain protections for e-commerce users' personal information. However, in order for CPTPP members to take into account certain elements in the language of international organizations, there is no standard that should be brought in terms of legal procedures, except for the general conditions of be more specific, a party may fulfil certain responsibilities by accepting and enforcing policies such as privacy data protection, business-specific bridge laws, and privacy-related laws, and laws that enable the execution of voluntary contracts by connecting to the interface. By just personal. Some members of may also be invited to support their data protection type management skills.[34]It is also always paid in full for privacy protection. This US-driven agreement, only records some weak and missing protections, but can be transferred to the EU-US at the time is bound by the Safe Harbour Protocol Schrems I Decision of the Court of Justice of the European Union (CJEU),

3.4 The OECD Legal frameworks

The Organization for Economic Cooperation and Development, which also known as OECD[35] which is an international organization comprising countries, It mainly works as a negotiation or proposal for the comparison of the policies of, solving mutual problems mainly through the recognition of the market and checking the domestic and international laws of member states regarding progress, equality. time and health of members of the state. Cooperation between European countries, including Canada and the United States, was also seen and developed in the 1960s, the main focus of which was to increase a country's economic growth and development. However, the aim of the organization is to support the policy that will improve the living conditions of people.[36]The regard to, the OECD has good policies in the organization and its employees must conduct their work transparently and in accordance with to ensure that personal information is protected externally. This is a very good check of and the actions of member states also check accordingly.

Finally, OECD guidelines on the protection of privacy and the cross-border flow of personal data play an important role in the international legality of the system. The second part of the law sets out eight principles that the government should use, which show the process of collecting, storing and cleaning information at the level. or shared without legitimate reasons. One of the principles of is that the person receiving the contract must be honest about information regarding the work to be performed.

In addition, that people have the right to access personal information and have the right to request errors, the information is removed by allowing any form of corruption, and major is necessary or desirable. There are also

[34]Article 14.8(5) CPTPP.

[35] http://tesi.luiss.it/30017/1/136363_TREMATERRA_CLAUDIA.pdf

[36] Wafa Tim, 'Global Internet Privacy Rights – A Pragmatic Approach University of San Francisco Intellectual Property Law Bulletin' Volume 13 of May 3 2009, Page 131-159, OECD www.oecd.org.about.OECD "Better Policies for Better Lives", http://www.oecd.org/about/.

some tips. The report has some important uses. Justice sets out principles of transparency and fairness. Although there is no relationship between these principles, they must have an impact on national and international law to promote and protect the information of private documents, since they are considered to be practices of specifically with the evolution of information protection.[37]In order to improve the level of protection, although it is necessary to change this structure to meet the protection needs of brought by the advancement of new technology in modern communication, which has led to changes in society, and legislation should be prepared developments in your surroundings to safeguard information..[38]

Even for strengthening the level of protection it is very much necessary to update these kinds of principles to meet them closer to the needs of defence coming from the advancing of new kind of technologies in a modern communication network, which contribute to the changes of a society and also legislation which has to find themselves to be ready to face the new developments which take place in the surroundings.

3.5 UN Development:

It has a long history of endorsing the right to privacy from its human rights treaties, but which mainly from article 12 which is provided under UDHR (universal declaration of human right)&also comes in Article 17 which comes under(international Covenant on Civil &Political Rights) ICCPR. UN is also the one which strengthen its role in privacy protection too high profile of measures which include,

- Firstly, the publishing of the declaration on digital rights
- Secondly which also has the option to provide private information under Privacy Policy.

Statement provides the Declaration asserts the right to privacy in the digital age we live in, and in December 2013 the United Nations General Assembly expressed its deep concern over this negativity and adopted Resolution 68/167. Observation and communication will be more. The checking & interruption of communication which may be more common.[39]This also recognized that the rights people have offline must also be protected online, and urged all countries to respect and protect the right to privacy in digital communications. The General Assembly also recognizes that offline human privacy rights must be protected online and therefore encourages by International Conference that brings all states together, unlike communication which reviewed the procedures, practices and laws regarding the oversight of the language to the International Human Rights Law regulations. The resolution notes, which involves the international law on human rights which provides the worldwide framework against which any kind of interfering to privacy of information of an individual rights which essential get evaluated. The international Covenant on Civil and Political Rights which need to be get rectified by almost

[37]Z. Torrey, 'better policies for better lives', IP Law Bulletin OECD P:20-30

[38] Peter Blume, Peter Seipel, Ahti Saarenpää, Dag Wiese Schartum, Nordic 'Data Protection', IustusFörlag, Uppsala 2001 Page:40-50

[39] United Nations, Resolution adopted by the General Assembly on 18 December2013https://www.itu.int/en/ITU-D/Regional Presence/UN/Documents/GA_Resolutions_ICTs/ares71d212_en.pdf

187 states who also provide that none shall be subjected to arbitrariness or any kind of illegal interfering with his or her privacy which may involve in family, home, or correspondence and not any illegal attacks upon honour and reputation very much. It has also much stated that everyone has their own right to be protected of the law against any such kind of interfering or any kind of attacks. There are also other international rights for human on intrusions which contains same kind of requirements. But right to privacy under international rights of human law which is not very much absolute with an occurrence of intrusion which must be subjected to key, full and critical valuation of its requirement, lawfulness and also proportionality as well. This kind of a determination which was surveyed by a detailed report which conclude and involve the practices in many of the states have discovered a lack of satisfactory national law making and enforcement weak procedural safeguards and also, infective oversight which involve all to be contributed to a lack of accountability for arbitrary or any kind of unlawful interference in the right to privacy.[40]

The special rapporteur which is a term which is independent expert which get appointed by the UN Human Rights Council to examine and also to report back on a specific kind issue which need to be regulated. In July 20 15 the Human Right Council who appointed the special rapporteur on right to privacy. The appointment which has the fix term for three years onwards.

The special rapporteur which is much mandate by human rights council resolution are as follows:

❖ Firstly, gathering the relevant information which may include upon international and national contexts, national applies and also experience to study kind of movements, growths and issues in relation to the right of privacies. It also makes some kind of recommendation to ensure its promotion and protection which may include in linkage with the issues rising from the new kind of technology usage.

❖ Secondly, by seeking, receiving, and responding to information while avoiding duplication from states because of which UN and its agencies program and also funds by regional human rights mechanism which may include national of human rights commission of institution, society of civil organisations. and the private sector, which involve business, enterprises and also another relevant stakeholders and parties under it.

❖ Thirdly, the possible identified cycles to the promotion and to the protection of the right to privacy identify exchange and also to promote principles and also best practices at the national, regional and also at international level, and also to submit kind of proposals and recommendations to the Human Rights Council in that regard, which may also include a view to the particular challenges which means arrives in the digital age.

The strength and the limitation for UN initiatives which may involve that it has the wide respect and also global coverage around the world. It has also the long history of promoting and protecting human rights in larger way in any issues which may arise. It has also a recognition of privacy as a fundamental right onwards.

The limitation of UN which may involve that the current treaty which are too high level for day-to-day impact for which right to privacy needs to be get translated into much further detailed principles also. The other limitation is that UN faces some kind of significant resources constraints onwards.

[40] UNHR, High commissioner for human rights on the right to privacy in the digitally www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx Page-30-40

3.6The convention of Council on Europe

The Data Protection Commission was established in 1981 under Convention

and is also known as Convention of Council of Europe or CoE, the most important and binding international data protection agreement of Convention of the data protection. The Convention was established by the Council of Europe, but is open to accession. It is on its way to membership by any country and members who have signed the Convention among some non-European countries are on their way to the Council of Europe. The Convention is on its way to reaching members of the Council of Europe. There are some legal protection documents, 46 out of 47 members of the Council of Europe Amended Convention are a party to the Convention, the exception being Turkey, where the convention was brought to the Turkish Parliament in the country has enacted its data protection law. Even in the 2013 Uruguay Round, in which the first non-European countries were party to the meeting, other countries are seeking participation.

Finally, the Convention operates through a collaborative, open process. It depends on the tool that supports state integration. This conference is heavily supported by other similar initiatives and was also created by the International Data Protection Board and is the best international standard.

The limitation of Council of Europe convention which involve that it has a Eurocentric history by although it is now being rapidly expanded all over the world. It is also faces some kind of possible challenges in accommodating very different national schemes, but most importantly with the US. If we see overall, then the Council of Europe Convention which is most promising international developing in a field where every kind of initiative which faces significant problems.

3.7 Initiative in International Data Protection Commission

Data protection has an almost universal initiative working at

international data protection authorities. Their model or main role is

, the data protection laws of many countries, but their work is more than

international conflicts, which are involved in the emergence of the global privacy debate.

.International Data Protection Commission which also have theme male initiatives which are:

- Firstly ,meeting annually basis and conference happened.
- Secondly, organization which happen for cooperation in the international and crossing territories which complaints side by side.
- Thirdly, a statement which is upon global privacy principle to be regulated.

In 2005, the International Data Protection Commissioner issued a statement titled "Protection of Personal Data as Privacy in a Globalised World", citing the Montreux Declaration on the Respect for Diversities and a frame working. The Declaration, also called the International Convention on Data Protection, is one of the most significant efforts to harmonise data protection laws around the globe. Specifically, the Declaration stated that Data Protection and Privacy Commissioners can express their will to strengthen the international recognition of the universal character of these principles in a large way.

Eventually, Governments and international organizations and supranational organizations agree to cooperate in a specific way, to establish general conventions for the protection of individuals who process personal data on a large scale leaders also called for a number of methods.

The commissioners who also appealed in various ways such as:

❖ Firstly, the UN should prepare legal instruments with human rights that explain the principles of data protection and special rights.

❖ Secondly governments around the world are promoting the use of data protection and privacy policy tools as a data protection protocol, and some of the continue to do well.

❖ Thirdly the European Commission (also known as Article 108 of the Convention) and non-party states pursuant to article, article 23 of the Personal Data Protection Convention on the automatic processing of personal data. Council of Europe The European Commission believes that already has data protection rights to comply with Convention and its additional recommendations.

Strengthening of the (International Data Protection Commissioner's) IDPC whose initiative included which is the significance of global influence and also profile of the Data Protection Commissioner's. in the real world where the experience and insight comes into the current issues comes in data protection. It also involve the emphasis on the Council of Europe Convention which is a global platform where rather something or propose of anything new comes.

The limitation of International Data Protection Commissioner's whose initiative involvement of the most significant a lack of formal structure or any follow up and the other one is the non binding of nature of the declaration onwards.

CHAPTER 4

LAWS RELATING PROTECTING DATA

4.1 Introduction

The law which has established the right to privacy under international law. But privacy which referred as most basic rights which use as fundamentally by which every individual who are much entitled and provide protection.[41]

The privacy principal, which is the core and the most important principle which mainly found much easily under Article 12of (Universal Declaration of Human Rights), UDHR and also under their privacy rights which were given formal legal kind of protection under Article 17 of (International convenient on civil and political rights), ICCPR and the protection of an individual of personal sphere which is very much provided. This kind of protection which has not been strong. But some kind of scholars which has shown that by type and numerous negotiating history between both UDHR and the ICCPR that the right to privacy which mainly under the umbrella term, which almost accidentally found its way into the treaties and was also data enshrined and comes under the national constitutions for the security of the data. As time passes, the international guidance for the protection of data privacy, which has privacy greatly of extended due to effects of new the technologies threats, and may bring new ways to protect data. though even the Human Commission Rights has not yet certain been emerged, biased issues may arise. The law, which has analysed its important aspects such as the protection of personal data or information against both public authorities and private entities, must be equally protected. Data subjects must be informed about the processing of their data and have the right to correct or eliminate any unlawful teams or any inaccurate data.

In 1990 United Nation on General Assembly who has also adapt some of the regulations from the regulation of computerised personal files of data where they keep them guidelines have required some minimum assurances to include certain key principles of data protection, such as lawfulness, fairness, accuracy, purpose specification, adequacy relevance, and of data collection and processing for data as security. Even though some of the guidelines are non-binding, they state that certain principles may be departed from for reasons of national security, public order, public health, morality, and the right of others. Even more recently the appointed UN special Rapporteur on the right to privacy in which discussion of his efforts to develop some kind of international legal instrument regarding the surveillance and privacy which not as such materialised also.

[41] GA reference in 217 (III) A(UDHR Universal Declaration of Human Rights), art12 https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_217(III).pdf

4.2 Laws on data protection

Evolution of the digital trading system which is required to protect personal data with the help of some kind of privacy policies..[42]Even if a piece of personal information is considered a commercial product, some business rules must be made with using a privacy policy. In this section, the importance of the right to privacy of personal data and its annex is explained briefly.

Some of the regulations which are phenomenal has its own origin in a possible violation of internal or external peace[43]. But according to Polcak and Scantess on who has the two sort of risks as direct and indirect which are connected with the present information which may also involve infringement which includes of a single sovereignty, peace on internet, and the right to let singular which create some kind of forward coming of risk also. Some kind of infringement which basically moves set of single data which has the most unnoticeable effects of group manipulation of social manufacturing as well. This information is used for control purposes in an environment with no material or personal impact. It is very difficult to remove this data, because there are possible situations in which such a malfunction can be found in the process of protecting personal data.

Although the international community with objective problems sometimes finds this problem difficult to solve, this problem is not easy. This section examines privacy policy in trade agreement CPTPP (the Comprehensive and Progressive Agreement for Trans-Pacific Partnership) in trade in services agreement and the work of exporters and importers between OECD and APEC (Asia-Pacific Economic Cooperation). Information on the protection of personal data GATS. Even now, the release of GDPR(General Data Protection) in 2018 outpaces legal issue

.However, this article will not do more about it. Although it has no impact on countries outside the EU Union, the protection of confidential information is a big problem even if the scope of application is only the EU confidentiality.

.

4.2.1 OECD Privacy Guiding principle

The organization for Economic Cooperation and Development, which adapted the OECD 2013 guidelines which are related to privacy which make the kind of demands related to the new digital trading era. These guidelines include that of the utmost are importance protecting the privacy of data in privacy guidelines also suggest that under the government who should not overcontrolling or interfere with the cross-border flow of data.[44] Even the OECD, which promotes the respect for privacy as a fundamental value and condition for the free flow of personal data across borders, has recognized the importance of privacy and with

[42] Malcolm Crompton and Peter Ford 'Implementing the APEC Privacy Framework: A New Approach', IAPP (International Association of Privacy Professionals) available https://iapp.org/news/a/2005-12-implementing-the-apec-privacy-framework-a-new-approach/

[43] Article 17 ICCPR.

[44]Michael Donohue, Billy Hawkes, 'Personal Data Protection at the OECD' OECD Privacy Guidelines (2013) available https://www.oecd.org/general/data-protection.htm

which the concern also comes is that of a growing number of online entities or threats whose main focus is to collect major amount of personal data get gathered. But to harmonise the privacy regulation among its members, the privacy guidelines which also develop some kind of basic principle for national application need to be regulated. Even some phrases of the principles which included in the OECD privacy guidelines which also further get advanced from time to time.

Most of the information regarding personal data is limited to and must be obtained with the knowledge or consent of the data controller by law most state the purpose and subsequent use must be limited to or incompatible with the achievement of those purposes. Subject to limitation, personal data will not be disclosed, made available or used for purposes other than those specified in, unless authorized by the data subject. Personal data must be protected by security measures to prevent the risk of data being lost, inaccessible, destroyed, altered or disclosed elsewhere.

OECD Guidelines Controlled Exporters and Export Information, which also addresses the relationship between individuals and knowledge management.

Information communication about the person entitled to consent from the data controller and data controllers as to whether the data controller has information. Finally, personal data must be protected by some security Savickas against any risk of loss of access, restriction, use, modification or disclosure from other sources that may steal personal information. The data controller is responsible for following the work numbered, which is valid for the previous model. In addition, should be responsible for any personal data under their control, regardless of the location of the data, so that even cross-border data is protected..[45] Even the Council also recognises that member countries have some kind of common interests in promoting and also in protecting the fundamental values of privacy of an individual liberty and the global free flow of information throughout the cross border.[46] Now nationally coordinated strategies which is mainly to accomplish some kind of right balancing between the social and economic assistances of data and analytics also.[47]

4.2.2 APEC security

APEC Privacy Security Framework was established in early 2015 to facilitate e-commerce in the Asia-Pacific region. Complies with the 2013 OECD policy as well. [48] It may also provide a framework that includes or relates to the protection of data. However, according to the OECD process provides too much freedom to send information. APEC members are more interested in blocking large information flows to run trade on an international trade-based scale.

[45]Australian Law Reform Commission, OECD WHICH INVOLVE POLICY ISSUE OF BARRIER ON TRADE AND AGRICULTURE TAD/TC/WP (2014)final

[46]Ibid

[47]Ibid

[48]*APEC Privacy Framework (2015)*

This will also realize the great potential of e-commerce, most will only focus on business expansion and reduce the cost of use economy.[49]Consumers, businesses and governments will benefit greatly from this process, which supports local information. The main purpose of APEC privacy is to suggest that members should avoid certain restrictions on posting additional information so that information is freely accessible. This kind of a framework which enables a local data from transfers will benefit consumers, businesses and also government in large way. APEC privacy framework main focus is to promote that the members should avoid the certain kind of unsigned accessary barriers to information to flows through freely.[50]This framework contains the Privacy Policy, according to which people are blocked. Some comparisons with OECD rules are not strictly necessary .But APEC lets merchants decide whether to keep

information, which is a denial of the fact of. According to APEC Article 9 and 19, there are two articles about element Article 9 is fundamental according to APEC, which means that the role of must be knowledge-based. However, the Chrome redirection and referencing this principle is the key difference between the APEC framework and the EU Border Management Policy. This kind of framework which includes principles for privacy, protection under it.

Under APEC in which principal 9 is a central which means that an accountability should follow the data.[51] But according to Chrome turn and forwarding this principle is the most important difference between the APEC framework and the EU directive on border controls policy. Even while framing once an organization who has collected information which may remain as an accountable for data weather that kind of may remain domestically or internationally or in both ways. This kind of principal is important because it may realise upon the protection of data itself and involvement of the parties for example persons itself who are involved and the collector involved under it. This is how the framework does not create any kind from border barriers to restrict the information to be get transferred.

Then comes the principal 3 within which by framing, which may involve collecting of information which should be much restricted to an information that is much relevant to the purposes of collection and any such kind of information should be obtained by lawful means which may be appropriate, with such kind of notice or consent of an individual to be needed.[52]The such kind of exception of this rule, which found in a principle for, which allows the collection of a personal data through the consent of an individual whose personal information is collected when necessary to provide. Kind of service or product which requested by an individual or required by a law under it.[53] But the furthermore the principal 5 which states that an individual who have the certain right to

[49]*APEC Privacy Framework (2015)*

[52] *A*PEC Privacy Framework (2015), Principle 3 available https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1

[53]Principle 4

exercising a choice about the collecting of news and also to disclosure of their personal information which may provide the case in the present information publicly happening.[54]

The APEC requires privacy framework which only in cultures the cross border cooperation between members of it. This kind of framework which may also include type of mechanisms to assist in investigations and also to identify and also to prioritise kind of cases for cooperation in surface cases of privacy infringement also.

There have been some kind of arguments against this kind of framework by calling it 2 weeks in the Protection of Privacy. As for instances Professor Graham Greenleaf, who argues that it has a kind of bias towards the free flow of personal information. This kind of requirement of accountability coupled with a requirement either of consent are that the disclosed takes. Reasonable steps to protect the information which is set to be very soft as compared to the EU directive.

But as on the other hand also the APEC privacy framework which respond to the social kind of factor is required only to protect the individual once they have traded with their data because it gives them protection to the data which is the most important concept but which also allows the data flow which also responds to kind of factor behind personal data.

4.2.3 CPTPP Guidelines

CPTPP is a free trade agreement covering 11 countries, of which are part of the Pacific region, including Australia, Mexico and Canada. This is an example of how free trade agreements protect personal data, but at the same time to time or movement may require its members to allow cross-border data flow to further facilitate certain transactions. But according to Deborah Elms of the Asian Trade Centre, the CPTPP is the most important deal we've seen in two decades along way.[55]

CPTPP, which Article14.8 of CPTPP, which contains a section on electronic commerce, where the article protects personal data. Parties in recognition of economic and social benefits and cooperation in protecting personal information of e-commerce users. This enables to increase customer confidence in e-commerce in large way.[56]

Then Article 14 requires all parties to apply the laws framed in order to protect the credit information and personal information of commercial users in electronic commerce. They should also consider some of their terms and guidelines on privacy protection. There will also be because all parties should support the development of the process to facilitate the relationship between the different controls. Accordingly, this process may include the recognition of climate control. accorded autonomously or by any mutual kind of arrangement, or by any kind of broader international regulatory. There are some other kind of relevant Article which is 14.11 in which for the cross-border transfer of information by any kind of electronic means comes under it. It may involve It can belong

[54]Principle 5

[55]A.F, 'What on Earth Is the CPTPP', The Economist available https://www.economist.com/the-economist-explains/2018/03/12/what-on-earth-is-the cptpp

[56]Chapter 14-Electronic Commerce, in Consolidated TPP Text (Government of Canada, 2016) availablehttps://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng

to any party and have its own rules. They must allow the cross-border transmission of data, including personal data, by electronic means, if these activities are for the purpose of performing the business of the affected person.

4.2.4 GATS Guidelines

General Agreement on Trade in Services, which includes the Protection of Personal Data. GATS is an operational framework through which all kinds of digital changes occur. It has World Trade Organization (WTO)rules that affect the information passing through it. The freedom to choose your own privacy protection rules is also a necessary end.

Eventually Finally XIV as a general exception to Article XVI the government must take certain measures to protect the privacy of individuals, process and disclose personal information confidentiality, ethics, public order, health and fraud prevention are among the reasons for controlling the data flow, which is also mentioned in the regulations within the scope of a policy objectives. The GATS may contain basic principles of information flows, or at least core business objectives. However, according to Tuthill, capital flow can be compared to information flow of information. This also recognizes that data is an integral part of the service.

Article I, referred to the addition of paragraph 2 (c) in which promised to allow all capital transfers in his territory. Even if members allow cross-border information flow. However, there are people who not sure about, as information, which is the most important part of the service, can be defined as

capital when itself cannot be defined. This means that this file can also be defined as a service type that needs to be modified as needed.

Types of commerce comes in the WTO. This shows that there is no clear information about water flow in most of the countries. This can become a challenge for modern business and traditional business in the world of flowing of data through cross borders. Even if there is an international agreement, the focus should be on creating a law no.

to regulate the trade of personal data. The international community should support the digital economy by not consolidating the flow of personal data, but by bringing together, but establishing some appropriate legal frameworks and protecting the business on the long run to protect data of the traders. Individuals may also use the Privacy Policy as a protection that can be used at any time. The biggest difference is right to keep information confidential and right to keep personal. But that principle, volente non fit injuria, there is a law that applies in this case, then there is a law that limits the defence to what interferes with those who are entitled to the defence consents to the violation of their personal data.

4.3 CASES

1.Office of the Privacy Commissioner for Personal Data v/s Octopus[57]

The Octopus group of companies provides smart-card payment services and a rewards program in Hong Kong (China). In 2010, as a result of growing public concern (and also revelations by an informant), Octopus was discovered to possibly have been selling personal information of customers to third parties for marketing purposes. It was suspected that Octopus sold information of approximately two million customers, gathered through the applications for its rewards program. After Octopus finally admitted to transferring the data, the Office of the Privacy Commissioner for Personal Data launched an investigation and produced findings. The findings confirmed that Octopus' actions violated several data protection principles contained in the Personal Data Ordinance; however, the Commissioner decided that an enforcement notice was not necessary in light of the circumstances and certain corrective commitments made by Octopus. Many consumers were disappointed that no punishment occurred, and the Ordinance was subsequently amended in 2012 to be less lenient with regards to direct marketing. The amended Ordinance includes stronger consent provisions, a mandatory opt-out opportunity, and a specific procedure that must be followed before personal information is disclosed. Fines for failing to comply were increase to a maximum of $1 million (HKD).

2.The Benesse data breach Japan[58]

July 2014, after advertisements had been sent to Benesse customers from a separate IT company, Benesse announced that millions of items of customer information had been leaked as a result of a data breach. The information related to children and their families, and affected tens of millions of customers. It was later found that a systems engineer contracted from an outside fi rm had breached the Benesse system by copying the information onto his smartphone device, and later selling the information. Japan's Personal Information Protection Act (PIPA) is primarily focused on policing the handling of personal information by businesses. After the incident, Benesse issued compensation in the form of cash vouchers to its customers, and committed to handling system maintenance in-house. The incident also prompted the Japanese Ministry of Economy, Trade and Industry to investigate Benesse's security procedures, and to consider amending its guidelines with respect to data security. The case, in combination with another large data breach by Japan Airlines, prompted widespread concerns that the previous data protection law was ineffective. In 2015 the Government upgraded and strengthened the legislation; the new law will come into force in 2017.

[57]Office of the Privacy Commissioner for Personal Data v/s Octopus (Hong Kong, 2010)
[58]The Benesse data breach Japan, 2014

3.FTC v/sTRUSTe[59]

On March 12, 2015, the FTC filed a complaint against True Ultimate Standards Everywhere Inc (TRUSTe) for alleged violations of , Section 5 of the Federal Trade Commission Act trust and certification company TRUSTe provides certification that meets the needs of its client. TRUSTe holds a variety of privacy and security certifications, including the EU Safe Harbor Trustmark. Companies may also appoint TRUSTe as complaints handler. The complaint claims (in part) that TRUSTe rejects requirement for user certification and recertification while TRUSTe claims that the program requires annual recertification, the FTC claims that there were no annual reviews for more than 1,000 times between 2006 and 2013. The FTC claims that this practice has resulted in false &misrepresentations to consumers. The complaint also alleges numerous other false and misleading statements made by TRUSTe. In the matter was settled, TRUSTe agreed to pay $200,000 and TRUSTe was subject to various obligations regarding the conduct of business. This document demonstrates the need for monitoring and regulatory control received by intermediaries such as TRUSTe.

4.S v/s Microsoft[60]

This case deals with the question of whether a warrant, sought under Section 2703 of the Stored Communications Act (SCA) and issued to law enforcement agents of the United States, may be used to obtain information stored on servers outside of the United States. The case is ongoing and is widely considered as a key test of the 'balance' between law enforcement access and individual privacy. Microsoft owns and operates a variety of web-based services, including e-mail services. Communications are stored in one or multiple of Microsoft's data centers, some of which are located outside of the United States. In this particular case, law enforcement agents of the United States sought the search and seizure of "information associated with a specified e-mail account" that was "stored at premises owned, maintained, or operated by Microsoft." Microsoft complied with the SCA warrant with regard to information held on servers in the United States, but moved to quash the warrant to the extent that it required the retrieval of information located on a server in Dublin, Ireland. A federal magistrate judge refused to quash the SCA warrant, on the basis that it applied to information stored outside of the United States. The court asserted that "it has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information." In examining the elements of extra-territoriality, the court refused to apply the 'presumption against territorial application'. The presumption provides that where statutes are silent on the issue, as was the case here, extra-territorial reach does not exist. Instead, the court pointed to legislative history and practical implications, finding that "an entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad in connection with a criminal investigation." This case has important implications with regard to governmental requests for information. It sets

[59]FTC v/sTRUSTe (US, 2015)

[60]S v/s Microsoft 2014 to 2015, US

a precedent that ignores the physical location of data, and focuses instead on the entity in control of the data. The practical implication, as illustrated by this case, is that United States law enforcement agencies may obtain digital information that is located outside of the United States if it is controlled by a U.S. registered company. The case is now the subject of an appeal.

5.FTC v/sAccusearch[61]

This case provides an interesting example of cross-border cooperation. Accuse Inc. was a company doing business as Abika, operating a website that provided information search services, which could target and profile individuals. Accussearch would forward search requests to third-party researchers, and would then relay the results back to the client as an intermediary. The case against Accuse was initiated by the Canadian Internet Policy and Public Interest Clinic (CIPPIC), based at the University of Ottawa. CIPPIC noted that although based in the U.S., Accuse actions affected Canadian citizens. CIPPIC first lodged a complaint with the Office of the Privacy Commissioner of Canada (OPC), who initially doubted that its authority extended to policing organizations physically located in the United States. CIPPIC then fi led a complaint with the FTC based on violations of U.S. law, and encouraged the OPC to coordinate with the FTC. Both the FTC and OPC ended up pursuing Accuse through coordinated efforts. The FTC provided the OPC with evidence of Canadian individuals being affected by the company's actions, while the OPC fi led an amicus curiae brief supporting the FTC's case in the United States. The complaint noted that some of the searches provided detailed phone records, which are a category of information protected in the United States by the Telecommunications Act 1996. Since telecommunications companies are forbidden from disclosing this information, the acquisition of the information "would most inevitably require someone to violate the Telecommunications Act or to circumvent it by fraud or theft." The FTC successfully brought a suit against Accuse in the United States. The 10th Circuit Court of Appeals confirmed that the FTC has wide latitude to pursue and prevent unfair practices, because the Federal Trade Commission Act generally prohibits "unfair or deceptive acts or practices in or affecting commerce". An unfair practice can be anything that "(1) causes or is likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers themselves, and (3) not outweighed by countervailing benefits to consumers or to competition.

6.Belgian Commission for the Protection of Privacy v/s Facebook [62]

This This is the first instance of country law in data protection law. At the time of writing this research is an objection. After Facebook changed its privacy policy in 2014, the Belgian Privacy Commission (Committee) launched an investigation and found Belgian universities for review. On March 31, 2015,Katholieke Universiteit Leuven and Vrije Universiteit Brussels published their final report entitled "From Social Media Services to Social Media Services: A Critical Analysis of Facebook Amendment Rules and Regulations". Report shows several

[61]FTC v/sAccusearch (2009, US)

[62]Belgian Commission for the Protection of Privacy v/s Facebook (Belgium, 2015/2016)

practices that Facebook would violate Belgian data protection law in further, the court found that the execution of as contrary to a security advantage and was also unfair as was not adequately sanctioned. Facebook appealed the decision; however, agree no. 04/2015 The station that could mark the end of the "single EU controller" model adopted by many companies operating in Europe "From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms," was released on March 31, 2015 by the Katholieke Universiteit Leuven and the Vrije Universiteit Brussels. The report outlined several of Facebook's practices that were potentially in violation of Belgian data protection law. Facebook has appealed the decision; however, if Recommendation no. 04/2015 stands, it could signal the end of the "single EU controller" model that many companies operating in Europe have adopted.

CHAPTER 5

COMPARATIVE ANALYSIS OF DIFFRENT COUNTRIES

5.1 INTRODUCTION

The most analysis which involve the effect of agreements which happened in trade on information on governing and by practicing in a local manner. It also concluded that the credit agreements can limit the scope of countries to arbitrarily imposes restrictions, for example as a disguised restriction upon international trade and also outside defying public policy objectives by which extent to search kind of agreements can act as distance evolve by spending on the making some of the policies or regulations.

This may involve the more of information of which may expand and some of links to be used for restricting the information on data usages in some of the countries who may use in illegal manner then may by presenting and by evolution of kind of effect which may made some of the policies usage. The select many of the countries. This may use as an analyse under European union which may reflect some of the light upon selecting some unique patterns which may relate to the European union or united states or may also involve united states of America who are the largest of partners hand in hand for developing of the some the privacy.

Although most of the analyses in the nature of data and type sections provide an analysis of the nature and rationale of territorial arrangements for data in these areas. In addition, examines the types of impact on local knowledge and on the contrary, the cross-border effects of freedom of information. Regardless, we need to present regional information as an increase in regulatory restrictions on the cross-border movement of goods and services. The intuition of the data flow helps move the business to the right. This is a situation in which the differences in the production processes of many countries are common, especially with the emergence of cross-border costs as the main driver of international trade. Join the high integration of services and more than products. In this type of competition, the purchase of cross-border trade increases by to interact with the price in the simulation book on cross border trade which add to treat cost in a kind of a manual analogous to traffic and tariff and non tariff kind of majors also.

5.2 The kind to represent details of the modelling approach.

Although most of the analyses appearing in the Nature of Data and Type sections provide an analyse societal requirements for data in these areas. In addition, examines the types of impact on local knowledge a on the contrary, the cross-border effects of freedom of information.

It is some changes in regional data show changes in the services of Organization for Economic Cooperation and Development local.

To capture our main steps are as follows The key steps which are as follows.

❖ To capture the impact of changes in some information in the change, use the absorption method with the involvement of SDRI, which has become one of the most important workflows from the change.

❖ The most effective method available includes information technology and Communications and other businesses, often including or enabling storage, Business, financial services, etc. and more others with added value and fashion including activities eg cars, electric motors and computers. Such sectors classically show a high degree of service and goods integration

❖ Most effective method which may given in the data to be intensively by involving the businesses like Information Technology and telecommunication which mainly include or enable the kind of storage, business, financial services and many more as well.

Other one is the high value added and fashion, which includes activities such as automotives, electrical machinery and computing also. This kind of sectors which classically display on high degree of integration between services and goods only.

The type of modelling which involves measuring the impact of a policy that changes relative to a baseline and focuses on cases by analysing

kind of effect upon data information which may relate to the policies by governing them as not a statically basis and also in a certain deed which may currently subjective to be reviewed and revised upon it. It may also very much presently sure on both ways like in internationally and also at national level onwards.

Some of the approaches as related are:

Firstly, the model which may get effected by certain interest by the countries or by power partners who may move from certain kind restriction of policies which comes under across territory of the border to flowing of a data which may also get stored in overseas which may be not to be get stopped. Such kind of approach which may has several kinds of analysis like:

- The flowing of data information through cross borders which may have certain methods which may create some kind of pressure in favouring of some locally only. This may comes as completion way or may be as conditional way.
- This may also come out from a specific FTA which involves certain current regulations and provide a large amount of the scription to some of the nations to go in a directions for localization of the data which involves the types of problems they set on cross border information flowing.

Secondly which includes over all starting kind of restricted setting which describe in by above any one of problems, by which the modern of hypothetical surrounding where the countries may have some of like and then EU ended in the agreements which is bilateral which can secure flowing of a data information much more freely.

5.3 Analytical analysis with the countries

5.3.1 India

India identifies as a realistic method for data protection. India alone does not have data protection laws, but has protections available in laws, regulations and guidelines. The most important section is in the Information Technology Act 2000, and was amended by the Information Technology Reform Act 2008. Specifically, relates to Section 43A, Security Privacy Policy and Procedures
and has been added by Information Technology as Security Policy and Privacy Policy or Regulations2011.
Finally, the scope and service of these units is very broad Limited
• Providence in general only applies to personal information only
• This provision is limited to some participating sites for data processing
• Customer only it can comply with the law numbered on a small number of regulations.
Finally, to solve these problems, India decided to implement the Medicines Act
for a time. The Privacy Act 2014 is a government decreed law but the exact process is not clear yet. There is currently no central, national or regular or independent agency in India to protect data.
However, the Data Protection Act bill under review will establish a national Data Protection Authority (DPA) in India. There are also restrictions on the transfer of sensitive data offshore Data will only be sent to countries where sensitive data will be adequately protected Data Technology Required Security and Procedures and Data Information Regulation 2011. Sensitive data is also
defined under Law regulation 2011 as information on data documents with content including passwords, financial information, health information, medical information personal biometric information.

5.3.2 China

The legal framework of China is very much back governing and across territorial of boundaries through which information regarding data can be transferred by localization which is a kind of patchwork of certain many laws and rules which may involve some type of national standards. Despite the complexity of the legal framework, this kind of implication is much. This may come as an exception to most parts. China thus has the best restricted policies on a crossing borders data flowing and this is a kind which is not limited to personal data. China cyber security lobbyist was passed in November 2016 a cyber security law which is the most expansive and fundamentally legal laws concerning the data to be protected through internet.

Chinese cybersecurity lobbyists passed the Cyber Security Lawin November 2016, the most comprehensive and important law covering information security on the internet. The law refers to the country's current law for cross-border documents as a practice. This may also include personal or sensitive information
that cannot be transferred before leaving China. This complete security assessment will require approval from the relevant authorities for the transfer of

information. It is controlled by issues related to national security, development work, and promoting the translation of information for the public good to society. Law covers all network employees, but there are special provisions for CII employees.

The scope of CII ownership is defined by supporting documents and the Cyber Security Act. These include sectors such as finance, electricity, media, telecommunications, utilities, defence and technology. All network operators must go through security measures before sending data abroad. This security assessment should consider national security, public interest, and the security of personal information. CII, Carriers capable of transferring documents abroad must be supervised, but must locally maintain copies of personal and important documents that can be sent worldwide.

In addition to the general transfer information listing the number in China, there may be a Tata localization. Provide information on private business purposes only from 2011People's Bank of China issued a statement on foreign mergers

Processing and storage of personal financial information of Chinese citizens similar to private economic activities involving non-personal information. For example, insurance department and some healthcare institutions in China that provide storage services and process data for transmission only. Additional regulations in China are even banned in foreign countries; This includes Internet services mapping of some kind of personal database, including which is limited to merchants in China.

5.3.2.1 Relation of trade with public policies

China's main focus is the information management framework for public policy issues, especially the area code security system. China, world data governance has poor data, most reasons. The desire to ensure network security and then national security. Security, these important questions, mainly for important matters, some questions may include the benefits of export business, subject to those who want to keep questions and as much discretion as possible. The success of goal in managing the flow of information to achieve its goals.

China believes that in addition to its national security concerns, information

is an important strategy for national security and has value in upholding the law of considered useful on its own, this is one which include National Science and Technology "13th Five-Year Plan" main purpose documents, mainly focus on data protection. It also joins the knowledge space to support this goal by helping businesses in China faster on the highway. China also has fewer restrictions on data protection when it comes to moving data across borders or regions

which is more in line with its general policy on the Internet. China also has the ability to exert some kind of local control over the Internet, with being considered the best replaced by other countries. China may also use some data management features of digital services. It is stored only in the Chinese market and only in the national border.

5.3.2.2China Free Trade Agreement

China has also signed up to the Regional Comprehensive Economic Partnership
(RCEP), which includes provisions on information localization and information border crossing. However, the contract structure of shows that the agreement not only has a strong points, but also limits China's resources, where the Special text of materials can be determined by itself. The types of items covered by
are:

Article 12.14(2) must have local tools question is only about doing business in one country. Section 12.15(2) Section also prohibits the cross-border transmission of information. This is not required for the implementation of
services. However, there are some of the two rules checked and balanced that are only legally allowed. Some documents territorial regulations, restrictions on public legitimate purposes, including cross-border transit, and restrictions on the reasonableness of certification non-technical procedures or not applicable in our case but confidential non-commerciality.

These provisions, which are used in other trade agreements such as the CPTPP and WTO provisions, are provisions of varying importance for the future.

But just as importantly, it's up to the signatories to decide what needs to be done to protect their legitimate interests. Doing so is difficult, but not impossible, if one of the other parties to the RCEP opposes the unnecessary measures taken by the other districts. This means that China and all other signatories will have ample room for to continue to share and manage their data at regional scale and even cross-border data regardless of the provisions of Articles 12.14 (2) and 12.14 (3). Stable relationship partners of regional trade. This is also the price change required for China to sign the deal first with certain kind of commitments.

5.3.3 France

France is a good example of the creation of for data protection, a data type provided by the representative of the European Union. But this would include some examples to use some is an interesting example using well complex registers. It may include DPA Article 66 1978, which was amended around 2004, which includes data protections of French documents, but the server has also passed another Laws with secondary protection information. Then there is the National Computer Science and Freedom Commission, also known as the National Commission on Information and Freedom. CNIL is independent regulatory body for the protection of privacy and personal information.

CNIL is also one of the most famous and active as with many other European data protection laws, some entries are required in Section 4of the Data Processing Act, which sets out the necessary procedures for data processing. It also depends on the type of data involved in processing, the data processing distance from four different Displays should be in accordance with

Data Processing Act 1978 for clearance. These rules are very complex. Permission is generally limited to the activities of our group that may affect privacy and freedom. Even in France, the content of the conversation with

data protection is CNIL, but according to the 2019 decree and in line with the findings of the European Court of Justice in the case SCHREMS I, which includes the CNIL with the highest power. Temporarily suspends international data and transfers it to the EU. However, incise he sent the matter to the Council of State. On the other hand, there is the Supreme Court numbered in France. The idea of such sufficient findings or other decisions of the European Commission number allowing the transfer of personal data outside the EU has been given.

Section 23 of the Data Processing Act 1978 sets out the most complex notification and consent requirements for cross-border transactions.

This includes changes that do not require notifications or any authorization within the EU. The second is for transfers only to countries declared eligible by the EU regulation. Requiring notification, and the third is for transfers to other countries where authorization is required.

5.3.4 Australia

Australia is a good example of the amendment that has expanded its privacy laws over the years by creating a new law with good help. The law still exempts some small business types and does not fully cover employee data, but is very close to international data protection standard. This privacy policy falls under the Privacy Act, which requires private entities to comply with the Australian Privacy Rules when collecting, using, disclosing and processing individuals' personal information . These laws were also significantly changed in 2012 in , which increased penalties and gave regulators the power of the last, which went into effect in 2014. government agencies and health customers. Australia's private legislation is also happily in line with EU Directive, Australia has never adopted all EU legislation apart from exemptions for document for small businesses and individual workers. Australia is a member of APEC and current privacy policy complaints about APEC's privacy policy. However, eventually

Australia is not a participant in APEC Cross-Border Security Policy Project APEC CBPR at this stage. The principal organizer is the Chief Security Officer in the United States. Level some states have been replaced by a similar institution. One of the key features of the Australian system is that there are no registrations for private entities under the Australian Privacy Act, but the international transfer of personal data is restricted if the organization cannot meet the requirements for certain configurations. These allow sample retention and data protection lawin the receiving country. includes giving.

5.3.5 Brazil

Brazil currently does not have a privacy law or data protection law, but is also a good example for a country that may try to create laws that protect information. Draft Personal Data Protection Billwas published in January 2015, but is only as broad as European Data Protection Directive. However, at the same time, the right to privacy is guaranteed by Article 5of the 1988 Constitution. Legislation also includes a new habeas corpus records right, which gives consumers the right to know what information is held with them and consumers to have this

information corrected. So, in addition to some of the restrictions added to privacy protection law, which can be found in Consumer Protection Act
of 1990, including the Brazilian Internet Civil Rights Act, 2014 Federal Act
, which gives the media more legal rights to Brazil.
The same is true for citizens and internet users. also applies to only personal data were sent to the country. This provides the same level of data estimates as Brazil's alone .As, noted in section 2 of this study by the Brazilian Consumer Association ,of these contain international data fields that are allowed to flow as long as they comply with 2014. But Brazil needs more regulation and
local standards. in this complicated world Professional Society of International Law Chamber. Brazil also missed the opportunity of to create a special organization for such problems and cooperate with the world for better management. applied for and defended the right to assembly. As always, Brazil decided in 2013 and 2014 in response to Snowden's injustice that some information in area should be given, but eventually ruled against it.

5.3.6 Indonesia

Indonesia is an exemplary country with laws showing the necessity of regional information. Information and Electronic Commerce Law 2008law related to privacy Article 26 on Business and Trade of Electrical Machines No. 82 dated 2012.Providing Additional Details. Electronic service providers providing
ensure the protection of the personal data they process. This protection generally includes obtaining appropriate consent and ensuring the security of personal data processes.
This protection generally includes obtaining the appropriate consent and ensuring that personal information is only used for a purpose, only for communication with the data subject. Indonesians do not lead by international standards. Indonesia is also a country that has not yet installed a data protection monitoring system in the country. While most laws remain silent on the creation of regulator, this will be addressed in future laws.
Indonesia is also one of the few developing countries, introduces a general regional information requirement affecting the information process for utilities only, Article1 of the Ministry Draft Regulation on Data Centre Technical Guidelines states: administrators can set up data centers and disaster relief centres in Indonesia. Then there is article 17 part 2 of Regulation of Electronic Transactions for Public Services, which is required to set up data centers and disaster recovery centers to protect the police and sovereignty of Indonesian countries and their citizens. , such rules are new, their effect has not yet been evaluated.

5.3.7 Japan

Japan is a country that recently revised its privacy laws to address certain concerns. Data which need the Protection of Personal Information, APPI 2003 has been applying for private businesses since 2005. This law covers public and private enterprises numbered. However, as a significant change to APPI, passed on September 3, 2015 and was not completed in 2017. But law is still in effect today, with a general exemption for foreign entities with fewer documentation because of the companies are certified as APEC CBPR participants, these

regulations may lead to exemptions for cross-border transactions under Japanese law of these regulations are enforced. Original Personal Information Protection Act, APPI, 2003these,did not establish a privacy management framework in Japan, but administrators assumed the role of privacy administrators dedicated to these offices.

This was also found to be a major flaw in the current system. The changes to APPI created a new privacy Policy Committee, PIPC, which will have significant review and inspection powers that require companies to submit their data compliance letter anonymous or collective. This work is included to promote and encourage the use of big data analytics in countries. While most EU standards apply to data transfers from local and international service providers, including for tracking subcontractors when data is transferred to three parties. While APPI Amending the Personal Data Protection Law of 2015 introduced more rules for cross-border transfers, also includes some exceptions.Japan's updated, which is considered a significant by improvement of submitting data processing monitoring.

5.3.8 Republic of Korea

Privacy laws in South Korea are contained in the 2011 Personal Information Protection Act, Personal Information Protection Act, PIPA ,as amended in 2013,2014 and 2015. The core principle of Personal Protection is based on a combination of EU directives. and OECD guidelines, which are about different. South Korea is also a member of APEC, but Courier does not at this stage agree with the other APEC cross-border privacy policy CBPR. But South Korea has a unique secret solution. If, among other things, users to suffer the same damage due to the organization's violation of data protection clause, the user can file a claim against the provider. In such cases, Service Provider will be liable for a will full of non-compliance or for negligence to cause any breach. Users can only claim damages that can be filed by the dispute resolution committee.

5.3.9 Russia

Russia has the Russian Privacy Law, which is complex and the main law is, and it is Federal Law. 15-FZ. The Personal Data Act of 2006 on personal data is supplemented by many additional laws, regulations, and directives, including:

First, processing and protection provisions block personal information
Information, created at the behest of the Federal Service Technology and Export Control Issue , February 5, 2010.

Secondly, Comply with the Government Decision dated 17 November 2007 and numbered 781,also established rules to ensure the security of personal data in the processing of personal data the basic processes of our organization are the basic processes and Personal Data Information System.

Thirdly the promotion of personal data security by organizing the support was announced on 15 February 2008.CombinedRussian law provides for the protection of confidentiality in all areas of life.

There are similarities between Russian legislation and EU directives. However, the application of rule appears to be limited. Russia is also a member of APEC, but does not participate in APEC cross-border regulations(CBPRs). But the detail of Russian law is the provisions of Article 10, number149-FZ of Federal Law No.of documents. Data protection technology and give the public the right to be forgotten and the ability ofto remove certain URLs from searches.

The main regulatory authority for this is office of the Federal Telecommunications Supervision Agency Information Technology and Mass Communications, Resonator. The country where the data is collected and processed must be registered in the employee data correspondence with Roscomnadzor. There are properties for simple one-time enrolments and HR records. Exporting abroad is the same as filling and processing domestically, and must be registered. Law of September 2015 requires data operators to store the personal data of citizens of Russia on servers in Russia. To enforce these laws, only Resonator fell in addition, a major foreign data operator, was given more time until early 2016 to comply with its policies. However, law
applies to data collection or was updated after September 2015.

5.3.10 South Africa

South Africa is a country with privacy policy, which is the purpose of the Privacy Act, which came into effect in August 2013. However, Bridge has the gap from the regulations covering all sectors. It is also a new example of the new privacy policy in the market. The policy also complies with and complies with EU Data Protection Directive. The Data Controller is one of the South African National Privacy Regulators, an independent body with the national
rights law.

5.3.11 United Kingdom

In UK in which DP[63] Act 1998 which is most important law for the people in surrounding and for the sectors which comes under privately. This may involve .The data protection act 1998 which implements the EU Data Protection Directive also. It also includes Article 8 of the Human Rights Act 1998,This is the most important rule for residents and private businesses. This includes the of which also applies in the United Kingdom. On the one hand, which respects the individual and family life, there is the right to family and communication.
Article is sometimes used for actions related to the struggle for freedom. But
Information Commission Office, ICO, is the UK's independent data protection regulator. Even data controllers must register with the Data Protection Office
Controller and apply for the required annual renewal to declare their intention to process personal data before starting to charge. There are minority exemptions that still have some records which is subject to various

[63] Data protection Act 1998

conditions, such as data protection laws allowing data to be transferred to non-EU countries, consent and agreements subject to them for the consent.

CHAPTER 7

CONCLUSION AND SUGGESTIONS

The different generation like the European Union, which take as the most important position to guarantee the protection of data personally of an individual and increase the privacy for an individual in trading system. The kind of system used globally by governing for which there are two kinds of protections of right provided which may bring a large protection by the EU legislative regime which may considered as an obstacle to the freedom of trade also. European Union, which has the legislation to protect the individual privacy and the personal data protection which is also guaranteed as fundamental human rights.

Even the most regulations which value a particular the General Data Protection Regulation, which also known as GDPR which may help in applying to all international commercial transaction concerning EU individual's personal data. It may apply to the business which are not conductive within the European Union. This may involve the suppliers in goods and also services in large ways this may also restrict the trade internationally because security in privacy and protecting of the data nationally.

This may also involve demand of protecting of data personally of suppliers so the data may not leak and get into hand of any third persons to use against them in large ways.

WTO and the General agreement on Information Privacy, which is a current situation that the WTO. It's not seeing as possible as it is to protect the data. There are some concerns about the about the privacy in case an international which might concern about the security service preferences and weaken the privacy protection worldwide also. The rules which are made is on other hand most important to regulate and protecting privacy of the trade in many ways.

The one who understood that the privacy protection which has clearly become the key topic for concern and for trade negotiation as well. There is also new and evolving rule making that seeks the rights and values of an individual socities in large. Most of the capacity which also go ahead in trading and also in innovating which has the most large demand in system for it.

The protection of data which need to one of the main priorities to be concern which is the most important for any nation whether it is personal data, national security data and many more as well.

SUGGESTIONS

- The international regulation related to the protection of data should be improved, regulated and properly executed.

- The international initiative on data protection in trade promoted by WTO, CPTPP, OECD etc should be effectively executed.
- There should be more effective laws on data protection system in India.
- While trading internationally the traders must ensure accurate information on their partners regarding doing business across borders whether they are trust worthy or not.
- The trader must ensure about the international law of the countries before trading.
- Traders must know and do depth research while trading because in international trade you never know that other party is trustworthy or not. Better be safe in trading than sorry.

BIBLIOGRAPHY

1.https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

2.LICRA *v. Yahoo* RG 05308 (May 22, 2000)

3.C. Kuner 'Regulation of transborder data flows under protection of data and privacy law- Past, Present and Future', OECD Digital Economy Paper No 187 of 2011 Page-, 680–685

4.S. A. Aaronson, 'Why Trade Agreements Are Not Setting Information Free: The lost history and debate over cross-border data flows, human rights and national security' World Trade Review vol 14(2015) page-672, 680–685.

5.OECD, 'privacy framework of supplementary of explanatory memorandum' Revised OECD privacy guidelines Paris: OECD, 2013.

6.J. E. Cohen, 'What Privacy Is For', Harvard Law Review 126 of 2013, page-120-123.

7.Mr. Joakim Reiter, Deputy Secretary General of UNCTAD, 'Data protection regulation and international data flows: implications for trade and development' www.unctad.com 19 April 2016.

8.The Economist, 'The world most value resource is no more oil but a data' in Economist availablehttps://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

9.Manyika, Mayer-Schönberger and Cukier, N. Henke .'The Age of Analytics competing in the data exclusion in the worlds' McKinsey Global Institute, 2016 Washington DC

10. R. Deibert., 'Access Contested: Security, Identity, and Resistance Asian Cyberspace' (Cambridge, MA: MIT Press, 2011) Page-11-20

11. Klaus Mathis, Avishalom Tor, 'New Developments in Competition Behavioural Law and Economics' Berlin Springer, 2019 Page- 241–263.

12. Irving A. Williams, Daniel R. Pearson, Shara L Aranoff United States International Trade Commission, 'Digital Trade in the US and Global Economies', Part 1,Page- 332-340(Washington, DC: USITC, 2013).

13. Anupam Chander and Uyen P. L'e, 'Data Nationalism', Emory Law Journal Vol.64 Issue.3 (2015), 677–739 www.emory.edu.com.

14. Article 7 Charter of Fundamental Rights of the European Union (CFREU) which distinguishes between the right of respect for private and family life and right to protect personal data under Article 8. https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

15. M. Burri and R. Schär, Journal of Information Policy 6 (2016), 479-511.Journal of Information policy by M.Burri and R.Sachr2016.

16. U. Gasser, 'Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy', Harvard Law Review Volume 130 Issue 2 December2016, Page 61–70. https://harvardlawreview.org/

17. CJ Bennett and also RM Bayley'Privacy protection in the era of the big data' Cambridge University Press https://www.cambridge.org/core/books/big-data-and-global-trade-law/global-trade-law-and-policy-in-the-age-of-big-data

18. I*bid*

19. Jennifer Daskal, 'Privacy and security Across Borders' Volume 128, Yale Law Journal, 2018-2019. https://www.yalelawjournal.org/forum/privacy-and-security-across-borders

20. APEC, Cross-Border privacy Rules System' https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules system

21. Joshua Paul Melttzer 'The internet, cross border data flows and international trade' Asia & Pacific Policy Studies, Vol 2 Issue1 page 90-102. https://onlinelibrary.wiley.com/doi/full/10.1002/app5.60

22. David Alexander 'Solution provide by Panetta on cybersecurity for national security' the Australian government by privacy commissioner ~~w~~www.privacy.gov.auon

23. FTCR REPORT 2012 on protecting privacy of a consumer available https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

24. World Bank, Pierre Sauve and Aditya Mattoo, Domestic Regulation and Service Trade Liberalization 2013 https://elibrary.worldbank.org/doi/abs/10.1596/0-8213-5408-6

25. Martin Abrams, 'The Strategic Front: Why Should We Care About APEC Implementation Privacy and Data Security' APEC L.*J* P- 22-34

26. Bruce Etling, Robert Faris and John Palfrey, 'Political Change in the Digital Age: The Fragility of Online Organizing Summer-Fall 2010 ' SAIS Review Vol. 30 no 2 Page-43-49

27. M. Burri, 'The International Economic Law Framework for Digital Trade', UNCTAD Volume 135 Page: 10–72

28. KORUS Annex 13-B, Section B available https://www.cbp.gov/trade/free-trade-agreements/korea/korus-implementation-instructions

29. Article 14.8(5) CPTPP.

30. http://tesi.luiss.it/30017/1/136363_TREMATERRA_CLAUDIA.pdf

31. Wafa Tim, 'Global Internet Privacy Rights – A Pragmatic Approach University of San Francisco Intellectual Property Law Bulletin' Volume 13 of May 3 2009, Page 131-159 OECD www.oecd.org.about.OECD "Better Policies for Better Lives", http://www.oecd.org/about/.

32. Z. Torrey, 'better policies for better lives', IP Law Bulletin OECD Page:20-30

33. Peter Blume, Peter Seipel, Ahti Saarenpää, Dag Wiese Schartum, Nordic 'Data Protection', IustusFörlag, Uppsala 2001 Page:40-50

34. United Nations, Resolution adopted by the General Assembly on 18 December 2013. https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy

35. UNHR, High commissioner for human rights on the right to privacy in the digitally P-30-40

www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

36. GA reference in 217 (III) A(UDHR Universal Declaration of Human Rights), art 12.

37. Malcolm Crompton and Peter Ford 'Implementing the APEC Privacy Framework: A New Approach', IAPP (International Association of Privacy Professionals) available https://iapp.org/news/a/2005-12-implementing-the-apec-privacy-framework-a-new-approach/

38. Article 17 ICCPR.

39. Michael Donohue, Billy Hawkes, 'Personal Data Protection at the OECD' OECD Privacy Guidelines (2013) available https://www.oecd.org/general/data-protection.htm

40. Australian Law Reform Commission, OECD WHICH INVOLVE POLICY ISSUE OF BARRIER ON TRADE AND AGRICULTURE TAD/TC/WP (2014)final https://one.oecd.org/document/TAD/TC/WP(2014)25/FINAL/En/pdf

41. http://tesi.luiss.it/30017/1/136363_TREMATERRA_CLAUDIA.pdf

42. APEC Privacy Framework (2015)

43. APEC Privacy Framework (2015)

44. APEC Privacy Framework (2015), Principle 9

45. A.F, 'What on Earth Is the CPTPP', The Economist available https://www.economist.com/the-economist-explains/2018/03/12/what-on-earth-is-the cptpp

46. Chapter 14-Electronic Commerce, in Consolidated TPP Text (Government of Canada, 2016) availablehttps://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng

47. Office of the Privacy Commissioner for Personal Data v/s Octopus (Hong Kong, 2010)

48. The Benesse data breach Japan, 2014

49. FTC v/sTRUSTe (US, 2015)

50. S v/s Microsoft 2014 to 2015, US

51. FTC v/sAccusearch (2009, US)

52. Belgian Commission for the Protection of Privacy v/s Facebook (Belgium, 2015/2016)

53. The Australian Government, The Office of the Privacy Commissioner www.privacy.gov.au/business/index.html

54. KORUS/Article23.1.2/.https//onlinelibrary.wiley.com/doi/full/10.1002/app5.60

55. Directive (EC) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of individuals with regard to the processing of personal data and on the free movement of such data.

56. https://www.cambridge.org/core/books/big-data-and-global-trade-law/global-trade-law-and-policy-in-the-age-of-big-data/DB1D911E8CB002EDDEAC168105ACFE83

57. Famously, F. H. Easterbrook, 'Cyberspace and the Law of the Horse', The University of Chicago Legal Forum 1996 (1996), 207–216.

58. art.7.https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-05782020000100087#fn66

59. Carlo Gamberale and Aaditya Mattoo, 'Domestic Regulation and the Liberalization of Trade in Services Development Trade and the WTO', Washington: The World Bank P. 290.

60. Martin Abrams 'The Strategic Front: Why Should We Care About APEC Implementation Privacy and Data Security' (2007) .privacy.gov.au/business/index.html

61. Bruce Etling, Robert Faris and John Palfrey Political Change in the Digital Age: The Fragility of Online Organizing' Summer-Fall 2010 SAIS Review, P. 37.

62. United States's request to China for information under paragraph 4 of Article III of the WTO General Agreement on Trade in Services.

63. Bernard Hoekman and Aaditya Mattoo (2008) Services Trade and Growth *World Bank Policy Research Working Paper 4461*, 3.

64. OECD Council Recommendation on Principles for Internet Policy Making(13 December 2011).

65. KORUS/Article23.1.2/.https//onlinelibrary.wiley.com/doi/full/10.1002/app5.60

66. OECD Internet Economy Outlook (2012) volume1 Page- 166

.

67. KORUS Annex 13-B, Section B

68. Jean-Francois Arvis, Yann Duval, Ben Shepherd and CorthipUtoktham) 'Trade Costs in the Developing World 2005–2010' World Bank Policy Research Paper 6309, P-6, 2011.

69. Andreas Lendle, Marcelo Olarreaga, Simon Schropp and Pierre-Louis Vezina (2012), There Goes Gravity: How eBay Reduces Trade Costs *World Bank Policy Research Paper No. 6253*, 19

70. https://www.cambridge.org/core/books/big-data-and-global-trade-law/global-trade-law-and-policy-in-the-age-of-big-data/DB1D911E8CB002EDDEAC168105ACFE83

71. Famously, F. H. Easterbrook, 'Cyberspace and the Law of the Horse', The University of Chicago Legal Forum 1996 (1996), 207–216.

72. G. C. Shaffer and M. A. Pollack, 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance', Minnesota Law Review 94 (2010), 706–799, at 715.

73. M. Burri and T. Cottier (eds), 'Trade Governance in the Digital Age the International Economic Law Framework for Digital Trade', Zeitschrift für Schweizerisches Recht' OECD 135 (2015), 10–72.

74. Article XIV(a) GATS.

75. Article XIV(c) GATS.

76. Article XIV(c)(ii) GATS.

77. e.g., G. Sacerdoti et al. (eds), The WTO at Ten: The Contribution of the Dispute Settlement System (Cambridge: Cambridge University Press, 2006). For the current crisis of the WTO dispute settlement,

see J. Pauwelyn, 'WTO Dispute Settlement Post 2019: What to Expect?', Journal of International Economic Law 22 (2019), 297–321.

78. Z. Torrey, 'TPP 2.0: The Deal without the US: What's New about the CPTPP and What Do the Changes Mean?', *The Diplomat*, 3 February 2018.

79. The definition of 'a covered person' in Article 14.1, which is said to exclude a 'financial institution' and a 'cross-border financial service supplier'.

80. The provision reads: 'Each Party shall allow a financial institution of another Party to transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business'

81. C-362/14, Maximilian Schrems v/s Data Protection Commissioner & Digital Rights Ireland Ltd, [2015]

82. http://tesi.luiss.it/30017/1/136363_TREMATERRA..CLAUDIA./pdf...

83. OECD, Wafa Tim, "Global Internet Privacy Rights – A Pragmatic Approach" Better Policies for Better Lives", University of San Francisco Intellectual Property Law Bulletin, Vol. 13, May 31, 2009: 131-159 http://www.oecd.org/about/.)

84. United Nations, Resolution adopted by the General Assembly on 18 December 2013, 68/167. The right to privacy in the digital age, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

85. 2014: The Study of the High Commissioner for Human Rights on the right to privacy in the digital age (A/HRC/27/37) United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age (an.Overview),..http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

86. http://www.dailysabah.com/politics/2016/03/26/turkish-parliament-passes-personal-data-protection-bill

87. The International Data Protection and Privacy Commissioners, Montreux Declaration - The protection of personal data and privacy in a globalized world: a universal right respecting diversities, 2005, https://icdppc.org/wp-content/ uploads/2015/02/Montreux-Declaration.pdf

88. https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=2596&context=jil

89. *OECD Privacy Guidelines (2013)*.
90. art. 7.https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-05782020000100087#fn66

91. *OECD Privacy Guidelines (2013)*, art. 9.
92. art. 10
93. art. 11.
94. art. 13
95. art. 13.
96. art. 14.

97. *OECD Privacy Guidelines (2013)*.
98. *OECD Privacy Guidelines (2013)*.
99. *APEC Privacy Framework (2015)*
100. *Malcolm Crompton and Peter Ford, Implementing the APEC Privacy Framework: A New Approach,* International Association of Privacy Professionals, December 01, 2005.

101. A*PEC Privacy Framework (2015), principle 9*
102. *principle 3.*
103. *principle 4*

WEBSITES

- www.unctad.com
- https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
- www.emory.edu.com.
- https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF
- . https://harvardlawreview.org/
- https://www.cambridge.org/core/books/big-data-and-global-trade-law/global-trade-law-and-policy-in-the-age-of-big-data
- https://www.yalelawjournal.org/forum/privacy-and-security-across-borders
- https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules system
- https://onlinelibrary.wiley.com/doi/full/10.1002/app5.60
- ~~w~~www.privacy.gov.auon
- https://elibrary.worldbank.org/doi/abs/10.1596/0-8213-5408-6
- http://www.oecd.org/about/.

- www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

- https://iapp.org/news/a/2005-12-implementing-the-apec-privacy-framework-a-new-approach/
- https://www.oecd.org/general/data-protection.htm
- https://www.economist.com/the-economist-explains/2018/03/12/what-on-earth-is-the cptpp
- https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng
- https://www.cbp.gov/trade/free-trade-agreements/korea/korus-implementation-instructions
- www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
- https://iapp.org/news/a/2005-12-implementing-the-apec-privacy-framework-a-new-approach/
- https://www.oecd.org/general/data-protection.htm
- https://one.oecd.org/document/TAD/TC/WP(2014)25/FINAL/En/pdf
- http://tesi.luiss.it/30017/1/136363_TREMATERRA_CLAUDIA.pdf