LUISS

Dipartimento
di Giurisprudenza

Cattedra di International Law

Right to privacy and personal data protection within WTO's digital trade policy framework

Prof. Christopher Michaelsen
RELATORE

Prof. Pietro Pustorino
CORRELATORE

Claudia Trematerra Matr. 136363
CANDIDATO

Anno Accademico 2019/2020

Table of contents

Introduction **2**

CHAPTER I - The Right to Privacy and Data Protection in International law ***9***

1. The Right to Privacy: the historical background **9**
1.1 Privacy as a Fundamental Human Right: an overview 10

2. Personal Data protection: an introduction **16**
2.1 Different definitions regarding personal data 17
2.2 Possible issues arising from data treatment 20

3. The Right to Privacy and personal data protection in International Law: an introduction **23**
3.1 Universal Legal Sources 25
3.2 Regional Sources 30
3.2.1. The Council of Europe Legal Framework 33
3.2.2 The European Union Legal Framework 41
3.2.3 The Organization for Economic Co-Operation and Development (OECD) Legal Framework 55
3.2.4 The Asia-Pacific Economic Cooperation (APEC) Legal Framework 56

CHAPTER II - International Trade Law and Restrictions on Data Flows under WTO regime ***61***

1. International Human Rights and International Trade Law **61**

2. The World Trade Organization: the historical background **63**
2.1 WTO structure 67
2.2 WTO sources of law 70
2.3 WTO functions 73
2.4 WTO Dispute Settlement System 75

3. Restrictions on Data Flows in International Trade: an introduction **78**
3.1 The application of GATS to Digital International Trade 81
3.2 GATS exceptions on free cross border data flows: an introduction 87
3.2.1 General Exceptions under GATS Article XIV 88
3.3 The obligations clauses under the GATS: an introduction 95
3.3.1. Most Favoured Nation Treatment obligation clause 97
3.3.2 The National Treatment obligation clause 100
3.3.3. Market Access obligation clause and Domestic Regulation obligation clause 101

CHAPTER III - Case Study: The application of GATS regime on GDPR Data Restrictive Provisions ***104***

1. Cross-Border Data Flows Restrictions under the GDPR **104**

2. Assessment of compliance of GDPR Cross-border data flows restrictions with GATS regime on obligations: an introduction **107**
2.1 Schedules of Commitments 107

3. Assessment of compliance of GDPR Provisions with the GATS General Exceptions. GATS Article XIV(a) and Article XIV(c) **116**
3.1 Assessment of compliance of the GDPR Compliance with GATS Article XIV Chapeau 121
3.2 International Trade Law and EU Law: how to coexist and to cooperate 122

CONCLUSION **127**

BIBLIOGRAPHY **132**

Introduction

The expansion of the internet and, consequently, the increasing use of communication technologies, have brought a rising awareness in the protection of personal data and in the advocacy of the right to privacy. In particular, in relation to digital trade, global data flows have assumed a vital importance, becoming the object of numerous international agreements and requiring a further protection of personal and sensitive data.

The thesis examines the relationship between the protection of privacy and personal data and international trade law. It focuses on how these regimes coexist and how they influence each other. In particular, due to the development of the digital service industry, governments have issued many measures limiting cross-border digital trade to protect their consumers and users. Many of those restrictions are data-protective measures, which consist in laws, regulations, policies, with the function to restrict cross-border data flows.

A major part of this thesis analyzes how international trade law and data-restrictive measures interact and to what extent they limit each other. It questions whether a balance between worldwide digital trade and the protection of the fundamental right to privacy and personal data is possible.

At the stage of this examination there is the potential conflict between EU restrictions on personal data transfer and the EU's non-discrimination commitments under GATS agreements. On one side, there is international trade law which promotes freedom of digital trade and consequently of data flows, while on the other side EU provisions limit the transfers of personal data outside the European Economic Area (EEA) to protect data and privacy of individuals. Such restrictions, in order to be lawful, have to meet a "necessity test" which consists in the determination of the opportunity of a certain provision for the effective protection of privacy.

The research shows that freedom of cross-border data flows, which is allowed by GATS commitments adopted by the EU, not only conflicts with the General Data Protection Regulation (GDPR), but also with Article 52(1) of the Charter of Fundamental

Rights of the European Union, which provides that derogation from the right to privacy and data protection are allowed only if necessary and proportionate.[1]

The thesis examines its causes and its possible remedies and, in conclusion, proposes the adoption of an international legislative framework regulating the right to privacy and personal data protection, in terms of avoiding possible conflicts of laws and to ensure fair and equitable international trade.

This thesis proceeds in the three parts. The first part will provide a comprehensive analysis of the developments made and the goals achieved in the protection of personal data and privacy in relation to the globalization and to the constant evolution of international (and digital) trade. It starts with an historical overview on the right to privacy, which has been recognized as a fundamental human right, finding acknowledgment in the Universal Declaration of Human Rights (UDHR) of 1948, in the International Covenant on Civil and Political Rights (ICCPR) of 1966, in the European Convention on the Protection of Human Rights and Fundamental Freedoms of 1950 and in the Charter of Fundamentals Rights of the European Union (EU), that took effect with the Lisbon Treaty in 2009.

The right to the protection of personal data has been frequently interpreted into the scope of the human right to privacy, also in relation with the private and family life.[2] It will be only with the Convention 108, which is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and with the Additional Protocol to the Convention of 2001, that the right to personal data protection has achieved a proper recognition, not depending on the context of the private and family life. Indeed, the scope of the Convention is the protection of both privacy and personal data.[3]

---

[1] Svetlana Yakovleva, "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'", *Journal of World Investment & Trade* Vol. 21 (2020): 881–919.

[2] Nadezhda Purtova, *Property Rights in Personal Data: a European Perspective,* (Kluwer Law International 2011): 224, 232–240; Perry Keller, *European and International Media Law: Liberal Democracy, Trade and the New Media* (Oxford University Press, 2011): 347; David Harris, Michael O' Boyle, Ed Bates, and Carla Buckley, *Law of the European Convention on Human Rights*, 2nd edition (Oxford: Oxford University Press, 2009): 362; UN Human Rights Committee General Comment 16, 23.03.1988, *UN Doc a/43/40*, 181–183 para. 10.

[3] Svetlana Yakovleva, "Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?", *World Trade Review* (2018), 17: 3, 477–508.

In the EU Charter of Fundamental Rights, the European Union promotes the right to respect for private and family life (Article 7 of the EU Charter) as well as a *sui generis* personal data protection right (Article 8 of the EU Charter)[4], thus conferring them the *status* of "constitutional" principles.

Moreover, these two rights are strictly linked, since Article 7 of the EU Charter finds its roots in Article 8 of the ECHR, which protects the respect for private and family life drawing, in turn, from the Universal Declaration on Human Rights.

The constant flow of personal data and the consequent need of protection of the individual's information and privacy is increasingly undermined by international trade and in particular by the digital services industry. In parallel with the developments of the services provided through the internet, the need to protect user information and data has increased and governments have been urged to find a way to limit the cross-border transfer of data through the application of restrictions on digital trades.[5]

This thesis intends to analyze the systems of restrictions on data flows, within both the EU and the WTO legal frameworks, and their relationship with the protection of the individuals' fundamental rights.

The second chapter of the thesis will provide an overview of the World Trade Organization (WTO) and of its sources of law, together with an analysis of the WTO provisions including restrictions on data flows.

The aim of WTO rules is to guarantee that international trade flows as easily, foreseeably and liberally as possible.[6] It this context, the General Agreement on Trade in Services (GATS) regulates the trade in services in the international legal system, and it is particularly relevant for the present analysis for what concerns data flows. GATS Members more and more deal with the consequences that data-restrictive measures have on the international digital trade.

---

[4] *Ibid.*

[5] Martina Ferracane, Hosuk Lee Makiyama and Erik van der Marel "Digital Trade Restrictiveness Index", *European Centre For International Political Economy, Digital Trade Estimates.* http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2018/09/DTRI-final.pdf

[6] World Trade Organization, "The WTO", available at https://www.wto.org/english/thewto_e/thewto_e.htm (accessed November 10, 2020)

Furthermore, Governments are allowed to issue data-restrictive measures in order to protect the privacy and the data of its users, and at the same time, GATS provides limitations on trades in line with those provisions.[7]

An analysis of the EU restrictive measures on data flow will be proposed, and in particular of the General Data Protection Regulation (GDPR) system, whose main purpose is to protect personal data and to promote that the fundamental rights and freedom of individuals can be invoked against the unlawful and unfair use of personal data.

The thesis will examine whether those protective measures may breach GATS obligations related to the Most-favoured-nation treatment clause, to the National Treatment clause, to the Market Access and to the Domestic Regulation clauses, or if they fall into the scope of the General Exceptions provided by Article XIV of the GATS. Indeed, it is explicitly stated in Article XIV(ii) of the Agreement that restrictive measures issued by Members are permitted if they are necessary to ensure the respect of domestic privacy laws.[8]

Those measures have to be proportional to the aim they intend to pursue and they have to relate to precise and objective standards of privacy and data protection in order to be in compliance with GATS. Indeed, GATS obligations are meant to inhibit disproportionate or prejudicial restrictions on cross-border data flows not to raise unnecessary barriers. Nevertheless, these obligations are valid only for those sectors which result in Members Schedules of Commitments signed under the GATS.[9]

The final chapter of the thesis is dedicated to a case study on the possibility of applying the GATS to the GDPR and in particular to those provisions related to the transfer of data. From an overview on the causes which may lead to a restriction of data flows outside the European Union, the study focuses on the adequacy mechanism, which is the instrument, provided by Article 45 of the GDPR, through which third countries are allowed to carry on business within the EU without suffering trade restrictions.

---

[7] Blayne Haggart, "The Government's Role in Constructing the Data-driven Economy", *Center for International Governance Innovation,* March 5 2018, available at https://www.cigionline.org/articles/governments-role-constructing-data-driven-economy (accessed November 10, 2020).

[8] Mishra Neha, "When data flows across borders: Aligning international trade law with internet policy objectives", *University of Melbourne, 2019,* available at https://minerva-access.unimelb.edu.au/handle/11343/233237 (accessed November 10, 2020).

[9] *Ibid.*

Although this mechanism may be found non-compliant to the MFN treatment clause provided by Article II of the GATS, it is argued that this mechanism can fall under the scope of GATS XIV(ii), and consequently those provisions can be considered justified and valid.

This research intends to shed light on the necessity to create a strong international legislation for the regulation of personal data flows across countries. Personal data are considered the extension of the personal sphere of the individual and they need to be protected with the same sensitiveness in which the individual as such is.

Personal data are proved to enhance digital trade and they have become an indispensable resource, making a major contribution to individual benefits, in relation to the production and the supply of services. Nevertheless, they take a back seat in relation to the risks individuals face when their data are (mis)used, running into identity theft, access to information by foreign and unknown authorities, forbidden access to websites or essential services, or also into less serious dangers like unrequested commercials, or personalized advertisements. Governments and authorities are aware of these undesirable possibilities and they act protecting data and people which retain a close connection with their State. It is mainly the States that must ensure the individuals' human rights and protect them from external negative interferences.

Trade in data, instead, being an international phenomenon, needs to be governed by universally recognised rules.[10]

The thesis raises the issue that is necessary to find a common point in the international community for the establishment of the rules and procedures to achieve a comprehensive enjoyment of those fundamental rights and freedom in trade.

Although it could be argued that the GDPR may be suited to become the global regulation in the area of personal data protection, the thesis shows that its provisions are not able to ensure the same opportunities to all the countries and it cannot satisfy the different needs of all the economies acting in the worldwide data interchange.[11]

---

[10] Svetlana Yakovleva, "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'", *Journal of World Investment & Trade* Vol. 21 (2020): 881–919.

[11] Bhaskar Chakravorti, "Why the Rest of the World Can't Free Ride on Europe's GDPR Rules", *Harvard Business Review,* https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules (accessed January 26, 2021).

Support for regulation differs significantly not only from country to country, but also within countries. For instance, some states may claim more stringent rules, but the same support may not be shared in other countries. This happens just in case of the GDPR which, for its compliance, requires high levels of data protection standards that not all the countries are able to afford, with the consequence for the latter of being excluded by the businesses.[12]

Sometimes, there could also be a difference between countries in the approach adopted towards privacy protection. For example, in the United States, there is the belief that the collection, analysis and selling of user data with minimal restrictions is an ability that companies have to achieve in order to become an innovative digital industry; an opposite position in comparison of the one of the EU countries.[13]

Thus, generally, the societal needs of balance between the right to ensure privacy and the pursuit of other benefits varies considerably and both users and companies will likely have to manage different rules for the various markets and technologies.

The problem arises when these different realities come into contact on the stage of international trade law. Indeed, since data is the currency of digital trade, the only possible solution to ensure a fair and free environment for the business is to establish a common legal framework governing the flow of personal information across boundaries.[14]

International policymakers have to cooperate to create independent and globally recognized regulations that find a fair compromise between local needs and global competitiveness, never abandoning the focus on the principles of privacy, transparency, and equity.

In conclusion, the aim of this thesis is to raise awareness of this topic among the experts and the international community, to stimulate the debate and to convince them that it is necessary to establish an international legislative framework regulating the right to privacy and personal data protection in the context of digital trade.

The project must include all the main needs of the States to guarantee a common level of privacy protection enabling all the actors to comply to the privacy standards

[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid.*

agreed, avoiding discrimination and unfair competition. The GDPR may be a starting point in just doing so, but there is still a long way to go.

CHAPTER I - The Right to Privacy and Data Protection in International law

1. The Right to Privacy: the historical background

The right to privacy is a crucial feature and concern of contemporary life and, throughout history and literature, privacy has been defined in different ways.

The meaning of the term "confidentiality" can be traced back to ancient Greek philosophers: Aristotle, in his political work, delineated an eloquent and memorable notion of what privacy was[15], making a distinction between the public sphere, *polis*, and the private one, *oikos*; he referred to *idios*, "private", addressing what was not of public domain, elaborating the concept of a sphere, conceived as a need, owned by each man, appointed to satisfy individual wills. Even at that time, property was considered inviolable, since it was believed that for a human being, to participate in public life, was simply necessary to have a place of his/her own.[16]

However, in the following centuries, the protection of privacy was conceived as a privilege of the bourgeois and not as a natural need of human beings.[17] During the years of the industrial revolution, along with the urbanization, the concept of "property" occurred[18].

Approximately, in 1890 the "Right to Privacy" came "officially" into existence, in particular, through the writings of two young lawyers, Samuel D. Warren and Louis D. Brandies, recognized as the "inventors" of the right to privacy. They co-authored the "*Right to privacy"*[19]*,* which has been defined as *"*perhaps the most influential law journal

---

[15] Judith A. Swanson, *The Public and the Private in Aristotle's Political Philosophy*, (Cornell University Press, 1992).

[16] Sergio Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, (Padova: CEDAM, 2006).

[17] Stefano Rodotà, "Riservatezza", *Treccani*, Enciclopedia Italiana – VII Appendice (2007), http://www.treccani.it/enciclopedia/riservatezza_res-9e2b210a-9bc7-11e2-9d1b-00271042e8d9_(Enciclopedia-Italiana)/ (accessed March 4, 2020).

[18] *Ibid.*

[19] Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy"*, Harvard Law Review,* Vol. 4, No. 5 (December 15, 1890): 193-220.

piece ever published".[20] Warren and Brandeis conceived the right to privacy as a common law right related to the personality of each individual, as an "inviolate personality".[21]

This means that every person has the right to decide what personal information should be communicated to others and to what extent. A distinction was made between privacy and the right to privacy, underlying privacy itself as a condition of the person, being in control of the "self" in the mental projection of other people.[22]

The article has gained an outstanding role, due to the development of privacy law at national, regional and universal level.

The purpose of this chapter, as it will be further discussed, is to present the developments made and the objectives achieved in the field of the right to privacy and personal data protection. The next paragraphs, in particular, are conceived to give an overview on some of the current legal sources regulating the protection of personal data, at universal and regional level.

1.1 Privacy as a Fundamental Human Right: an overview

In this paragraph and in the following one it is anticipated what will be further analyzed in the chapter, with reference to the international legal framework, universal and regional, on the right to privacy and the protection of personal data. In particular, this section aims at showing that, in the light of the legal instruments mentioned and described through the chapter (i.e UDHR, UN ICCP, ECHR and EU Charter), the right to privacy has acquired the status of a fundamental human right.

The next paragraph, then, serves to outline a general framework of the right to protection of personal data, necessary for the introduction and the connection with the paragraphs dealing with the specific topic of personal data, where the different notions of personal data and the possible issues arising from the processing of those data will be discussed.

---

[20] Allan P. Dionisopoulos, Craig Ducat, *The Right to Privacy: Essays and Cases* (St. Paul, Minn, West: Publishing Co., 1976).

[21] Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy"*, Harvard Law Review,* Vol. 4, No. 5 (December 15, 1890): 193-220.

[22] *Ibid.* at 216.

The right to privacy has been recognized as a fundamental human right after World War II, in the framework of the "International Bill of Rights project".

On 24 October 1945, the United Nations was founded, as the Charter of the United Nations was adopted. The main aim of this newborn international organization was to guarantee the maintenance of peace and security throughout the world[23], as the Preamble of the UN Charter states "We the peoples of the United Nations determined to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, and to reaffirm our faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small … have resolved to combine our efforts to achieve these aims."[24]

The United Nations' achievement was the realization of "a milestone in the history of human rights, a veritable Magna Carta making mankind's arrival at a vitally important phase: the conscious acquisition of human dignity and worth"[25], consisting of the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) with two Optional Protocols, the International Covenant on Economic, Social and Cultural Rights (ICESC) and its Protocol.[26]

The very first step taken by the United Nations was to adopt the Universal Declaration of Human Rights, by the General Assembly, on 10 December 1948. The declaration promoted fundamental rights, such as the right to life, the prohibition of torture and inhuman and degrading treatments, the right to equality before law, and, at a certain extent, the right to privacy.

Prior to the adoption of the Declaration, the right to privacy was solely promoted as an aspect of the right to respect the correspondence or inviolability of the home in national constitutions only. It did not exist, in any constitutional source of law, a specific

---

[23] Rhona K. M. Smith, *International Human Rights Law,* 8th Edition, (Oxford: Oxford University Press, 2018).

[24] United Nations, Charter of the United Nations, Preamble: "We the peoples of the United Nations determined to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, and to reaffirm our faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small … have resolved to combine our efforts to achieve these aims.

[25] OHCHR, The International Bill of Rights Fact Sheet 2, Rev 1.

[26] Rhona K. M. Smith, *International Human Rights Law,* 8th Edition, (Oxford: Oxford University Press, 2018).

promotion of the right to privacy, nor did the so-called "umbrella term" like "private life" or "privacy" under which the law of privacy could be guaranteed.

In the field of the right to privacy a unique phenomenon happened: privacy rights were recognized as a fundamental right at international level firstly, and then it has been enshrined in national laws.[27]

As it will be analyzed in detail in another paragraph of this chapter, privacy and protection of personal data have acquired the status of fundamental rights, firstly, through their recognition at universal level in the Universal Declaration of Human Rights (article 12) and, subsequently, in the UN Covenant on Civil and Political Rights (article 17).

In particular, Article 12 of the Universal Declaration of Human Rights specifically promotes territorial and communications privacy stating that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[28]

Article 17 of the UN Covenant on Civil and Political Rights mandates the right to privacy, too. It has been conceived to protect people against unlawful offences to their honour and reputation and to grant the protection of the law against such acts: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."[29]

Another step forward the recognition of the right to privacy as a fundamental human right can be seen in its promotion, at regional level, within the Council of Europe legal framework, which has the aim to promote fundamental human rights, democracy and rule of law among its Member States.[30]

---

[27] Kalin Walter, Künzli Jorg, *Universeller Menschenrechtsschutz*, 2nd edition, (Basel: Helbing Lichtenhahn, 2008): 4, 31; Christine Chinkin, "Sources", in Daniel Moeckli, Sangeeta Shah, and Sandesh Sivakumaran eds., *International Human Rights Law,* (Oxford: Oxford University Press, 2010).

[28] Universal Declaration of Human Rights, Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

[29] United Nation International Covenant on Civil and Political Rights, Article 17:" 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

[30] Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 1 (The Hague: Martinus Nijhoff, 1975): 20, 26; Alastair Mowbray*, Cases, Materials,*

The Legal Committee Rapporteur, French minister Pierre-Henri Teitgen, proposed in the first draft of the European Convention on Human Rights a provision concerning the protection of privacy, based on Article 12 of the UNDHR: "The Convention... will guarantee... to every person... [i]nviolability of privacy, home, correspondence and family, in accordance with Article 12 of the United Nations Declaration."[31]

The inclusion of the privacy provision, however, was not without obstacles. This was due to the fact that the United Kingdom was not opened to introduce provisions which may have the force of threatening its sovereignty[32] (a position which is confirmed by the fact that also the British Draft for the International Bill of Rights did not recognize the right to privacy).[33] Lord Layton, the British representative, particularly asked for the removal of the provision.[34] However, the Legal Committee did not approve the British request.[35]

In the second phase of the drafting of the ECHR, the Committee of Ministers asked the Committee of Experts on Human Rights to review the recommendations of the General Assembly and to establish its appropriacy of scope and content.[36] The response of the Committee of Experts was a Preliminary Draft Convention which contained a provision concerning the right to privacy almost identical to that one in Article 12 of the UDHR.[37]

Two alternative drafts were also provided as versions "A" and "B". The latter provided punctual definitions of the concepts of the rights promoted, specifically

---

and Commentary on the European Convention on Human Rights, 3rd edition, (Oxford: Oxford University Press, 2012): 2.

[31] Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 1 (The Hague: Martinus Nijhoff, 1975): 168.

[32] Ed Bates, *The Evolution of the European Convention on Human Rights, From Its Inception to the Creation of a Permanent Court of Human Rights,* (Oxford: Oxford University Press, 2010): 6, 77, 8.

[33] Oliver Diggelmann, Maria Nicole Cleis, "How the Right to Privacy Became a Human Right", *Human Rights Law Review*, 2014: 14, 441-458 *doi: 10.1093/hrlr/nguO4*. Advance Access Publication Date: July 7, 2014.

[34] *Ibid.* at 172.

[35] Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 1 (The Hague: Martinus Nijhoff, 1975): 220.

[36] Ed Bates, *The Evolution of the European Convention on Human Rights, From Its Inception to the Creation of a Permanent Court of Human Rights,* (Oxford: Oxford University Press, 2010): 79.

[37] Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 3 (The Hague: Martinus Nijhoff, 1976): 236.

mentioning the protection of privacy.[38] The former, instead, only enumerated freedoms and rights, without any references to the term "privacy".[39] The Committee of Experts could not decide between the two alternatives proposed and therefore it turned the work to the Committee of Ministers.[40]

A conference was held to discuss the alternatives and it ended with a New Draft Alternative B, characterized by punctual definitions and a space for privacy, left incomplete.

The final Draft did not contain an explicit reference to "privacy", but it introduced the umbrella term of "private life".

Finally, Article 8 was adopted on 4 November 1950[41] , which states that:

"Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

As we will see in another paragraph of this thesis, the European Court on Human Rights has given a broad interpretation of the terms contained in the article, including also the protection of personal data and the right to privacy.

In conclusion, it should be noted that another step forward the recognition of the right to privacy as a fundamental human right can be seen in the inclusion of a specific right in the Charter of fundamental rights of the European Union.

The EU Charter provides the full range of civil, political, economic and social rights which found their basis on the fundamental rights and freedoms recognised by the

---

[38] *Ibid.* at 312-320.

[39] *Ibid.* at 8.

[40] Ed Bates, *The Evolution of the European Convention on Human Rights, From Its Inception to the Creation of a Permanent Court of Human Rights,* (Oxford: Oxford University Press, 2010): 79; Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 4 (The Hague: Martinus Nijhoff,1977): 16.

[41] Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 7 (The Hague: Martinus Nijhoff, 1985): 46.

European Convention on Human Rights, the constitutional traditions of the EU Member States, the Council of Europe's Social Charter, the Community Charter of Fundamental Social Rights of Workers, and other international conventions to which the EU or its Member States are parties.

The Charter became legally binding on EU Member States with the entering into force of the Treaty of Lisbon in December 2009.[42]

Among the fundamental rights promoted by the Charter, the protection of the right to privacy and protection of personal data finds its space. These rights are guaranteed, respectively, in Article 7 and 8, which content corresponds to the one set forth in Article 8 of the ECHR.

In particular, Article 7:

"Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications."

(It can be noticed that consider the developments in technology the word "correspondence" has been replaced by "communications").

Article 8:

"Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the"

person concerned or some other legitimate basis laid down by law. Everyone has the right of access to

data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

In accordance with Article 52(3), the meaning and scope of these rights are the same as those set out in the corresponding article of the ECHR. This means that the

[42] Equality and Human Rights Commission, *What is the Charter of Fundamental Rights of the European Union?* https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union

restrictions which may legitimately be imposed on this right are the same as those provided by Article 8 of the ECHR.[43]

For the scope of this research this last topic concerning limitations in a crucial one, and it will be recalled further on and analysed in detail in the last chapter of the thesis.

2. Personal Data protection: an introduction

As anticipated above, the purpose of this paragraph is to present the topic of personal data and to highlight its importance in the modern digital world. In the next sections, instead, the subject of personal data will be introduced in a more technical way, with a focus on the different notions regarding personal data as long as on the issues that may arise from the treatment of the sensitive information.

Developments in information and communication technologies have revolutionized modern society; innovations in this field brought progress to civilization, but at the same time has led to concerns about the impact of modern technologies on individuals' private sphere and fundamental rights.[44]

Personal data can be defined as the whole of information regarding a certain individual, such as gender, address, geographical location etc. The value of each of those elements may also be associated with more than one person. This means that a set of information has meaning as it is then possible to associate or differentiate a specific entity from others.[45]

---

[43] EU Charter of Fundamental Rights, *Article 7*: "Everyone has the right to respect for his or her private and family life, home and communications"; *Article 8*: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data

[44] UNESCO, "Keynotes to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet", *United Nation Education, Scientific and Cultural Organization*, Draft Study, Connecting the Dots conference, Paris, UNESCO Headquarters March 3-4, 2015; Russell L. Weaver, David F. Partlett, Mark D. Cole, "Protecting Privacy in a Digital Age", in Dieter Dorr, Russell L. Weaver, *The Right to Privacy in the Light of Media Convergence: Perspectives From Three Continent,* (Berlin: De Gruyter, 2012): 1-30.

[45] James Waldo, Herbert S. Lin, and Lynette I. Millett eds., "Thinking about privacy: Chapter 1 of Engaging Privacy and Information Technology in Digital Age", *Journal of Privacy and Confidentiality*, Vol. 2, No.1 (2010): 19-50.

One of the biggest concerns of the digital age is personal data protection. New technologies are capable of having access, control and collect quantitative and qualitative amounts of information that would have been impossible to compile in the past.[46]

Today it does not take much more effort but one-click to collect information from an aggregated database. All devices connected to the Internet have their own and unique IP address, which make every connection trackable. The IP address can lead to the definition of a personal identity in many ways: for example, through the placement of intangible devices in a specific web browser, the website can easily collect all the information related to online activities. This operation is usually done through "cookies"- very small text files, created by websites, which are stored in users' computers to fulfil various functions, mostly to track and memorize users' preferences and information.

In this way the identification of a person may be deduced with the cross-examination of her/his activities, research, and in general from all her/his online behaviors. The IP address tracking method is just one of the million ways to collect personal information.[47]

In this framework, the Global Position System (GPS) also deserves a mention. It has the ability to detect the precise location of people and goods. This device is inserted as a default function in almost all electronic devices, so sending information about position and movement of people worldwide.

Another system used for data acquisition is the Closed-Circuit Television (CCTV), within which the video is transmitted. The circuit comprises of different elements such as the camera, recording devices and/or display monitors all connected with each other. Through CCTV cameras the governments manage to acquire a large amount of personal data.[48]

2.1 Different definitions regarding personal data

To find a definition of personal data, it can be useful to look at the EU General Data Protection Regulation (GDPR), since it provides for a series of definitions that

[46] Peter Carey, *Data Protection: A Practical Guide to UK and EU Law,* (United Kingdom: Oxford University Press 2015): 281-282.
[47] *Ibid.*
[48] I-Ching Chen, *Government Internet Censorship Measures and International Law,* (Wien, Zweigniederlassung Zurich: LIT VERLAG GmbH & Co. KG, 2018).

contribute to the creation of a framework by which the topic can be easily contextualized. The definitions provided by the GDPR are the result of a legislative evolution on the topic which started with the Convention 108 of the Council of Europe, and that developed with the issue of the Data Protection Directive.

The GDPR is the Regulation on data privacy and security adopted in the context of the European Union. It applies to all EU member States, and in particular to those organizations which target or collect data related to people in the EU.[49] Its main purpose is the improvement of data protection and the raising of privacy standards and according to the European Commission, it has to make Europe "fit for the digital age".[50]

Article 4 of the GDPR provides a series of definitions regarding personal data useful for the application of the Regulation.

It begins describing personal data as "any information that relates to an identified or identifiable living individual."[51] Thus, to fall into the scope of the Regulation, the storage of information, signs or indications has to be personal. This means that it should be possible, through that information, to detect a specific individual. Furthermore, data is personal if the identification could be done either directly or indirectly through the use of the information collected. This can happen, for example, when data is made of more physical or psychological characteristics, which combined with each other can lead to the construction of a unique individual identity. In the presence of certain details such as a person's name[52], an identification number or location coordinates, a personal profile can be created.[53]

---

[49] European Union, "What is GDPR, the EU's new data protection law?" *GDPR.EU,* https://gdpr.eu/what-is-gdpr/, (accessed March 4, 2020).

[50] Gráinme de Búrca, "New governance and experimentalism: An introduction. Symposium Issue on New Governance and the Transformation of Law", *Wisconsin Law Review*, Vol 2: 227-238.

[51] General Data Protection Regulation, Article 4.1 "For the purposes of this Regulation:
(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[52]Alexander Roßnagel, *Europäische Datenschutz-Grundverordnung Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts*, (Seiten, broschiert: Nomos 2017) Anwendungsbereich (2017).

[53] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR), A Practical Guide,* (Germany, Hamburg: Springer International Publishing AG 2017).

The GDPR proceeds with the definition of "processing". By that term is meant all operations conducted on personal data, carried on both with automated and non-automated means. This definition, offered by the second paragraph of Article 4 of the GDPR has been interpreted broadly so as to involve all the stages of the operations made with data, such as the collection, record, storage and also elimination of personal information. The two main reasonings behind the wide scope of the provision are the prevention of the risk of circumvention by companies and the intention to make the provision independent from the further changes of technology.[54]

In particular, specific processing conditions are ensured by the GDPR to special categories of personal data, which are considered "sensitive".

These personal data concern racial or ethnic origin, political opinions, religious beliefs, trade-union memberships, data related to the health, the person's sex life or the sexual orientation.

An innovation from the previous Data Protection Directive is the inclusion of "genetic and biometric data" among the sensitive ones. According to the wording of the Regulation, "genetic data" comprises all the information related to "the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question". By "biometric data", instead, reference is made to all personal data which are the result of "specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

A specific definition in the Regulation is provided also for data concerning health. These data are considered sensitive because they are related to the health status of a person, which is commonly recognized as one of the most private angle of an individual, suffice it to think about the medical secrecy. However, Article 4 No. 15 states that "data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

[54] *Ibid.*

In conclusion, in order to establish to whom the Regulation is addressed, the GDPR gives a definition of both controllers and processors. According to Article 4 No. 7, by the term "controller" reference is made to any natural or legal identity, public authority, agency or other body which "alone or jointly with others, determines the purposes and means of the processing of personal data."[55] The term "processor" refers to any natural or legal identity, agency or other body which is in charge to process personal data under controllers' guidance.[56]

2.2 Possible issues arising from data treatment

A relevant concern, through the issues that affect the protection of personal information, is the regulation of the electronic storage of data.[57]

The concerns about privacy rights from storage is exacerbated when databases are combined, for example when programs are developed in globally interconnected networks.

The memory size of storages allows for a massive stationing of data. Cloud computing, for instance, is a new technology through which users can store information on the Internet instead of a physical device. From one perspective this means saving data can be very effective and useful, from another it can badly affect the individual's privacy.

In fact, from the privacy angle, users lose control over their data as soon as they put their information on the Internet. Once storage systems gather information, those can be analyzed and used for various purposes, often far from those for which data was originally collected.[58]

An example can be found in "data mining": an automatic or semi-automatic program, which processes large amounts of information to create new connections of data elements or to find new patterns from separate and autonomous materials.[59] This process

[55] General Data Protection Regulation, Article 4 No.7.
[56] General Data Protection Regulation, Article 4 No. 8.
[57] James Waldo, Herbert S. Lin, Lynette I. Millett, *Engaging Privacy and Information Technology in a Digital Age,* (Washington, DC: The National Academic Press, 2007): 88-121.
[58] Christina Gagnier, "Regulating the Man Behind the Curtain", in *Future of the Privacy Forum, Big Data and Privacy: Making Ends Meet,* Stanford Law School the Center of Internet and Society (2013): 35-38.
[59] Usama Fayyad, Georges G. Grinstein, Andreas Wierse, *Information Visualization in Data Mining and Knowledge Discovery,* (San Francisco: Morgen Kaufman Publisher, 2002); Usama Fayyad, "The Digital Physics of Data Mining"*, Communications of ACM*, Vol. 44, Issue 3 (March 2001).

is used by political science researchers, or for social purposes without giving the chance to the data owner to express their consent upon their use.[60]

Another threat to the right to privacy could be represented by internet intermediaries - companies which have the scope to facilitate the use of the Internet, bringing together and facilitating transactions between third parties. These include internet service providers (ISPs), website operators and search engines. Increasing activity from such providers is raising a lot of concerns for the protection of individual privacy from the point of view of private entity interference and more specifically, the effectiveness of current regulations on the subject. These companies have at their disposal a large number of user information with the possibility to decide whether to safeguard the databases or to break all the user rights and freedoms by selling and exchanging data on the Internet.[61]

On closer analysis, ISPs are internet intermediaries, run by private entities, which have the role of offering services for online activities. Most internet service providers sell the information they collect (by doing data mining, analyzing users' tastes and interests), to companies or individuals. The majority of the time people have knowledge of the manipulation of their personal data.

Frequently, ISPs are forced to voluntary police user activities. The consequence is that the gathering of information can be used to not only monitor and uncover criminal activities, but also for completely different purposes such as eliminating dissenting opinions. Sometimes the intermediary is a state-own service provider; in this case the protection of people data is more challenging due to the difficulty in guaranteeing their transparency and government independence. [62]

Search engines can be analyzed to underline the different impact they have on people's right to privacy compared to ISPs. This role is played by companies such as Yahoo!, Bing or Google, which give Internet users the possibility to access an unlimited

---

[60] James Waldo, Herbert S. Lin, and Lynette I. Millett eds., "Thinking about privacy: Chapter 1, Engaging Privacy and Information Technology in Digital Age", *Journal of Privacy and Confidentiality*, Vol. 2, No. 1, (2010): 19-50.

[61] I-Ching Chen, Government Internet Censorship Measures and International Law, (Wien, Zweigniederlassung Zurich: LIT VERLAG GmbH & Co. KG, 2018).

[62] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Natalia Torres, "Global Survey on Internet Privacy and Freedom of Expression", *United Nations Educational, Scientific and Cultural Organization* (2012).

amount of information in few seconds. The service provider is an organized system which implements algorithms rapidly to connect to the information requested from a computer. Search engines carry on new privacy concerns as people, in exchange for the free search service, offer up their personal information to those companies. As a result, in the last few years, a number of worldwide protests have erupted for the protection of consumer's privacy. As Google, Yahoo!, Microsoft reacted to public concerns and in late 2008, a Global Network Initiative (GNI) was launched. [63]

GNI is a multi-stakeholder initiative where the Participants act to develop the Principles on Expression and Privacy (GNI Principles). Their scope of action consists of the direction and guidance of Information Communication Technology (ICT) whole industry to promote and protect human rights. It also provides standards to the ICT industry on how to develop user rights even when faced with government requests for disclosure of users' private information and censorship. The goal of this initiative is to ensure the transparency and affordability of its members' actions and to "respect and work to protect the privacy rights of users when confronted with governments demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards". [64]

The efficiency of GNI is ensured by the control over the implementation of the Principles every two years. The test consists of a review of specific case studies and by conducting a general company process review. The purpose is to establish if each member is "making good faith efforts to implement the GNI Principles with improvement over time". The activities of the GNI are conducted by companies with the help of academic experts, human rights groups and also socially responsible investors to better ensure the respect of standards for the protection of the right to privacy on the Internet.[65]

More and more companies, every year, are joining GNI and numerous social media, such as Facebook and LinkedIn, are taking part in this global action to promote

---

[63] Sergey Brin, Lawrance Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine", *Seventh International World-Wide Web Conference*, *WWW 1998*, (1998).

[64] Global Network Initiative, "GNI Principles on Freedom of Expression and Privacy" (2008), http://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf. (accessed March 5, 2020).

[65] Rebecca Mackinnon, *Consent of the Networked – The WorldWide Struggle for Internet Freedom,* (New York: Basic Books, 2012): 169-186.

and protect fundamental human rights on the Networks. This behavior has been seen as a sign of hope to help reinforce consumer trust.[66]

3. The Right to Privacy and personal data protection in International Law: an introduction

As analyzed above, digitalization has affected the entire society, interfering with almost any aspect of socio-economic relations and revolutionizing the ways in which people interfere and act, accessing, receiving and giving their information for personal and commercial purposes.[67]

These new behaviors have led human rights promoters to the acknowledgment that the protection of personal data on the internet is essential for the protection of dignity and integrity of individuals.[68]

Thus, the right to protection of personal data is one of those rights which belong to the most personal sphere of the individual, and it has been asserted along with the development of new technologies.[69]

The increasing importance of privacy and data protection issues has driven national and international "legislators" to deal with the new challenges arising from digital development, due to the fundamental status reached by data protection, which is enshrined within various constitutional instruments either as a separate right or as a part of the right to privacy. Worldwide legislators are engaged in the substantial and procedural protection of the right to privacy against unlawful and arbitrary interferences with individuals' private sphere.[70]

The protection of personal data requires that the collection, the use and the transfer of individual information can be conducted only behind the consent of the data owner, or

---

[66] The Global Network Initiative, "2014 Annual Report Protecting and Advancing Freedom of Expression and Privacy in Information and Communication Technologies", *GNI* (2014).

[67] World Trade Organization, "Trade Rules for the Digital Economy: Charting New Waters at the WTO", *World Trade Review* Vol. 18 (2019): S1, s121-s141.

[68] I-Ching Chen, *Government Internet Censorship Measures and International Law*, (Wien, Zweigniederlassung Zurich: LIT VERLAG GmbH & Co. KG, 2018).

[69] Pietro Pustorino, *Lezioni di tutela internazionale dei diritti umani,* (Bari: Cacucci Editore, 2019).

[70] I-Ching Chen, *Government Internet Censorship Measures and International Law*, (Wien, Zweigniederlassung Zurich: LIT VERLAG GmbH & Co. KG, 2018).

according to the law, which has to provide the transparent use of the data and also a proper balance among the interesses at stake (right to private identity, right to confidentiality, right to privacy, etc.). In order to ensure an adequate protection to personal data, norms and legislations have to take into account then various information and individuals involved; for example, data regarding children under 18 have to be strengthened their protection, as well as, the so called "sensitive data", consisting of information about the health, the political and religious opinion, the origins of a person, etc.[71]

Along with the protection of personal data, another right which belongs to the personal sphere of the individual is the "right to be forgotten". This is another right which has been asserted in concomitance with the evolution of technologies. It consists in provisions providing the complete removal of personal data collected. It has to be guaranteed not only when data are not needed anymore for the scope for which they were detained, but also when the owner of those data requires so, if those information are prejudicial the individual reputation.[72]

To date, according to the UN Conference on Trade and Development ("UNCTAD"), 132 out of 194 countries have adopted legislation to secure the protection of data and privacy.[73]

The next paragraphs are intended to investigate the current universal and regional legal sources regarding the right to privacy and data protection. From the comparison it could be noticed that, on a general level, data protection rules aim at regulating the conditions for collecting, storing and using individuals' information, trying to guarantee the people's right to monitor the treatment of their personal data, and providing remedies in case of breaches of norms and principles.

At universal level, within the context of the United Nations, a series of resolutions dealing with the protection of privacy in the digital age have been adopted, acknowledging that "the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital

---

[71] Pietro Pustorino, *Lezioni di tutela internazionale dei diritti umani,* (Bari: Cacucci Editore, 2019).

[72] *Ibid.*

[73] UNCTAD, Data Protection and Privacy Legislation Worldwide, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed on 1st May 2020).

age".[74] Moreover, it addresses to States, pointing out that they shall "take effective measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises".[75] Despite the non-binding status of UN General Assembly resolutions, they could represent a strong evidence of state practice and *opinio juris*.[76]

At regional level, instead, the instruments provided by the Council of Europe and the EU are quite advanced in the promotion of high levels of data protection while the ones coming from the Organization for Economic Co-Operation and Development and Asia-Pacific Economic Cooperation are more focused on self-regulatory approaches.[77]

3.1 Universal Legal Sources

As seen in the introduction of this chapter, privacy and data protection have been recognised as fundamental human rights firstly in the Universal Declaration of Human Rights and then in the UN Covenant on Civil and Political Rights.

In particular, the first Draft of the Declaration was presented by the Director of the United Nations Division of Human Rights, John P. Humphrey. In his paper, the "Secretariat Outline"[78], intending to give some basis to the work of the Drafting Committee, Humphrey included a specific provision on privacy, stating that "No one shall be subjected to arbitrary searches or seizures, or to unreasonable interference with his person, home, family relations, reputation, privacy, activities, or personal property. The secrecy of correspondence shall be respected."[79]

---

[74] United Nations, General Assembly, "The right to privacy in the digital age", Seventy-first session, Third Committee, November 16, 2016.
[75] *Ibid.*
[76] Stephen M. Schwebel, "The Effect of Resolutions of the U.N. General Assembly on Customary International Law", Proceedings of the Annual Meeting, *American Society of International Law,* Vol. 73, (April 26-28, 1979): 301-309.
[77] I-Ching Chen, Government Internet Censorship Measures and International Law, (Wien, Zweigniederlassung Zurich: LIT VERLAG GmbH & Co. KG, 2018).
[78] Drafting Committee on an International Bill of Human Rights, Report on its 1st Session, July 1, 1947, *E/CN.4/21* ('Drafting Commission Report 21') at Annex A.
[79] Drafting Commission Report 21, Annex A, Article 11. (Secretariat Outline).

The Drafting Committee for the Declaration modified that first provision as: "Private life, the home, correspondence and reputation are inviolable and protected by law."[80], emphasizing the first word: "private life".

It was not until the second Draft that the "umbrella term" came into existence. Even if the term "privacy" was conceived only to protect specific aspects of one's life: "The privacy of the home and of correspondence and respect for reputation shall be protected by law."[81]

However, with further iterations of the Draft, the previous reference to privacy was altogether eliminated, but when the Commission on Human Rights modified the Draft, it reinstated the umbrella term of 'privacy'.

On 10 December 1948 the General Assembly issued Article 12 of the Universal Declaration of Human Rights which included the following provision:[82]

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[83]

The aim of the Declaration was to urge States to improve their legislative frameworks and to lay down new procedures in order to guarantee an efficient human rights protection. It was conceived as an instrument of "soft law", and as such it has not a formally binding effects on States.

However, given the incorporation of the majority of rights included in the Declaration within subsequent international treaties, at universal and regional level, and national constitutions, it has been acquired the status of customary international law.

An example is provided by the US case of *Filartiga* v. *Pena-Irala*[84]*,* where it was proclaimed by the US Court that the Declaration had obtained recognition of customary

---

[80] Drafting Commission Report 21, at Annex D, Article 9. ('Cassin Draft')
[81] Drafting Commission Report 21, at Annex F, Article 12. ('Revised Cassin Draft')
[82] Universal Declaration of Human Rights, *GA Res 217A(III)*, December 10, 1948, A/810 at 71.
[83] Draft Universal Declaration of Human Rights, Report of the Third Committee to the 3rd Session of the General Assembly, Article 13, December 7, 1948: A/777 at 4.
[84] United States Court of Appeal, Second Circuit, *Dolly M. E. FILARTIGA and Joel Filartiga, Plaintiffs-Appellants, v. Americo Norberto PENA-IRALA, Defendant-Appellee,* No. 191, Docket 79-6090. Argued Oct. 16, 1979. Decided June 30, 1980.

law and as such it had assumed the force to prohibit torture under a specific customary rule.[85]

According to some legal scholars, for what concerns at least some of recognized the rights, they have acquired the status of jus cogens, category which enshrines peremptory rules which no State may derogate.

Furthermore, it has been in 1976, that the International Covenant on Civil and Political Rights (ICCPR) entered into force, being its provisions explicitly defined as legally binding for all the state-parties.[86]

Almost 20 years after the adoption of Article 12 of the Universal Declaration on Human Rights, in the ICCPR, Article 17 was inserted to protect the individual from interference with his/her family, home and correspondence, and directly to promote not only the right to privacy.

The said provision states that:

> "1. No one shall be subjected to arbitrary or *unlawful* interference with his privacy, family, home or correspondence, nor to *unlawful* attacks on his honor and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks."[87]

This article covers both unlawful and arbitrary interferences, referring to the States' duty to issue provisions for the specific protection of the right set forth in there. According to the term "unlawful", interferences may be authorized by states and only in cases provided by law, which itself have to be in compliance with the rights promoted by the Covenant.[88]

A further interpretation of this provision refers to the applicability of the wording of the Article 17 of the ICCPR to the collection and the storage of personal information

---

[85] *Ibid.*

[86] Martix Dixon, *Textbook on International Law,* 7th Edition, (Hampshire: Oxford University Press, 2013).

[87] International Covenant on Civil and Political Rights, Article 17.

[88] Human Rights Committee, "General Comment 16 (Twenty-third session, 1988)", *Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies,* U.N.Doc. HRI/GEN/1/Rev.1 at 21, University of Minnesota, Human Rights Library (1994).

on the internet or on digital devices, which have to be regulated by law, whether the operations are carried on by States, public authorities, private bodies or individuals.[89]

Moreover, in 1990 the United Nation General Assembly adopted a non-binding document with the Resolution 45/95, named "Guidelines for the Regulation of Computerized Personal Data Files".[90]

The document contains ten principles for the protection of data applicable both to national and inter-governmental organizations, which include *inter alia* the principle of lawfulness and fairness; the principle of accuracy; the principle of the purpose-specification; the principle of interested person-person access; the principle of non-discrimination; the power to make an exception; the principle of security; supervisions and sanctions; the transborder data flows and the field of application.

Furthermore, they set out the possible limitations on the transfer of data under the aim of the protection of privacy.

Paragraph 6 clearly states that "Departure from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedom of others, especially persons being persecuted provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system, which expressly states their limits and sets forth appropriate safeguards".[91]

These principles aim to ensure the protection of rights from public and private computerized files containing individuals' personal information. Each State and international organization have to implement its "legislation" following the basic framework for the processing of "personal data" given by the United Nations Guidelines.[92]

In 2018, the UN High Level Committee on Management (HLCM) stated personal data protection and privacy principles for the entire UN system.

---

[89] *Ibid.*

[90] UN General Assembly, "Guidelines for the Regulation of Computerized Personal Data Files", *A/RES/45/95,* December 34, 1990.

[91] *Ibid.,* para. 6.

[92] UN General Assembly, "Guidelines for the Regulation of Computerized Personal Data Files", *A/RES/45/95,* December 34, 1990.

They were published with the scope of giving some guidelines for the process of personal data to those who are carrying out their activities on behalf of the United Nations System Organizations. Private and public entities are working on the implementation of these principles in their programmes and policies. The Secretary General's new Data Strategy, to enhance the Members' commitment, has included in all the organization's operations, the integration of data protection and privacy. This policy has led to reforming works across the whole UN system.[93]

In 2013, the UN General Assembly adopted the resolution 68/167 on "The right to privacy in the digital age", which reports the restored international concern with regard to the human right to privacy and a commitment to United Nations (UN) institutions to investigate not only the meaning, but also the relevance, of this right in the latest digital age.[94]

The resolution achieves to the identification of the management on data as a human rights issue, highlighting the human rights influence of the cross-border data flows.[95] It encourages the states to take action in improving their policies and legislations through an efficient and innovative structure, in order to comply with the right to privacy. The recitals emphasise that due to the rising use of the Internet, there is also a rising possibility of violations of privacy by governments, individuals and companies.[96]

The resolution also stresses the consequences of the extraterritorial surveillance to the right to privacy. The assumption that international privacy rights are compromised by cross-border surveillance makes it tougher for governments to argue that there are no barriers for engaging in surveillance of foreign people outside the boundaries.[97]

---

[93] United Nations, "Reflection on Data Privacy", *Office of Information and Communications Technology*, https://unite.un.org/news/reflections-data-privacy. (accessed March 7, 2020).

[94] United Nations, "The Right to Privacy in the Digital Age", *United Nations Human Rights Office of the High Commissioner,* (accessed May 22, 2020).

[95] United Nations Human Rights, Office of the High Commissioner, "Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", *Human Rights Council*, *U.N. Doc. A/HRC/23/40*, April 17, 2013.

[96] United Nations Human Rights, Office of the High Commissioner, "The Right to Privacy in the Digital Age", *G.A. Res. 68/167, U.N. Doc. A/RES/68/167*, December 18, 2014.

[97] Colum Lynch, "Inside America's Plan to Kill Online Privacy Rights Everywhere", *Foreign Policy: the Cable,* November 20, 2013, https://foreignpolicy.com/2013/11/20/exclusive-inside-americas-plan-to-kill-online-privacy-rights-everywhere/ (accessed March 10, 2020).

However, the resolution does not state what an unlawful or arbitrary surveillance is, but it refers to the 2013 report by Special Rapporteur, La Rue, which affirmed that "limitations on the right to privacy must be provided by law, necessary in a democratic society, necessary to achieve a legitimate aim, and proportional, and must also limit discretion in their application and not impair the essence of the right".[98]

Accordingly, the international community has a duty to establish the terms under which the privacy of individuals may be jeopardised. Although the characteristics of such legislation or structures will be different, the Special Rapporteur's 2013 report provides some features that can lead to concerns from a human rights point of view.[99] The report highlights areas of concern as being insufficient judicial supervision, not well-defined national security exceptions, free access to data, the establishment of mandatory data retention laws, or of laws which restrict the use of privacy-enhancing tools.[100] Ultimately, one of the major concerns of the Special Rapporteur was to make clear that there should be laws providing that people have to be aware of the supervision and surveillance of their communications and data.[101]

3.2 Regional Sources

In order to further investigate the topic of the right to privacy and the protection of personal data, it seemed necessary to provide an analysis of the regulation of the main regional sources on the matter.

The starting point of the study is an overview of the legal framework of the Council of Europe. Defined as the "continent's leading human rights organization"[102], it has played a pioneering role in the recognition of the most fundamental rights and values. The most significant example of its work has been the adoption of the Convention for the

---

[98] United Nations Human Rights, Office of the High Commissioner, "Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", *Human Rights Council*, *U.N. Doc. A/HRC/23/40*, April 17, 2013: 29.

[99] *Ibid.* 54-62, 65-71.

[100] *Ibid.*

[101] *Ibid* 82-83, 91-94.

[102] Council of Europe Portal, *Council of Europe in brief,* https://www.coe.int/en/web/about-us/who-we-are (accessed January 5, 2021).

Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights (ECHR), which was opened for signature in 1950 and came into force in 1953. Its importance lies in the fact that it was the first instrument to give effect and to make binding some of the rights stated in the Universal Declaration of Human Rights.

During the years, the Convention has been amended several times and integrated with many other rights in addition to those set forth in the original text.[103] Among the rights guaranteed by the ECHR[104], there is the right to respect the private and family life, and as it will be analysed more in detail in the next paragraph, since this recognition has been crucial for the practical effectiveness of the protection of the right to privacy and of personal data. Regarding the latter, reference will be made also to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as Convention 108 too, a Treaty of the Council of Europe open for signature by the member States and for accession by non-member States. It was the first binding international instrument conceived to protect the individual against abuses which may derive from the collection and processing of personal data and to regulate the transfrontier flow of sensitive information.

Then, the focus of attention will turn to the sources of law of the European Union. In particular, the first one of the regulatory tools provided by the EU for the protection of individuals data was the Directive 95/46/EC of the European Parliament and of the Council of 1995.

Even if it is called Data Protection Directive (DPD), its official name is "Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data". It is a European Union directive which, as the name suggests, regulates the processing of personal data within the European Union. Due to its farsighted provisions, it has become a fundamental component of EU privacy law and, more in general of human rights law.

---

[103] European Court of Human Rights, *European Convention on Human Rights,* *https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c* (accessed January 5, 2021).

[104] Council of Europe Portal, *Council of Europe in brief,* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (accessed January 5, 2021).

A decade later, the Directive 95/46/EC has been superseded by the EU Data Protection Regulation.[105] It was on 25 January 2012, that the European Commission unveiled a draft European Data Protection Regulation[106], which became in 2016 the General Data Protection Regulation (GDPR).[107]

However, it was with the Charter of Fundamental Rights of the EU, that data protection and the right to privacy have been elevated to the status of fundamental human rights.

Furthermore, this thesis will analyze one of the international legal instruments provided by the Organisation for Economic Co-operation and Development (OECD). The OECD was provided pursuant to the Convention on the Organisation for Economic Co-operation and Development, to supersede the Organisation for European Economic Co-operation (OEEC), or the so-called "Marshall Plan", which was created in 1948 with the aim of reconstruction of the European economy after the World War II.

The scope of the Organization is to promote worldwide policies to strengthen the economic and social wellbeing of the peoples. A way to achieve its mission is through the promotion of the respect for privacy as a fundamental value and a condition for the free flow of personal data across borders. Indeed, in 1980 it established the first internationally agreed Guidelines set upon privacy principles. In 2013 it has been replaced by the OECD Privacy Guidelines**,** which are still in force. The main focus of this regulatory resource is the practical implementation of the protection of privacy in a global perspective, encouraging the interoperability among different countries legal instruments.[108]

The last regional source described in this chapter refers to the Asia-Pacific Economic Cooperation (APEC) privacy legal framework. The Asia-Pacific Economic Cooperation (APEC) is a regional economic forum established in 1989 to generate greater

---

[105] European Commission, Directive 95/46/EC, https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en (accessed January 5, 2021).

[106] *Ibid.*

[107] European Data Protection Supervisor, *The History of the General Data Protection Regulation, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=It%20replaces%20the1995%20Data%20Protection,their%20countries%20by%20May%202018.* (accessed January 5, 2021).

[108] Organization for Economic Co-Operation and Development, *OECD Privacy Guidelines*, https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm (accessed January 05, 2020).

prosperity for the people of the whole region by promoting healthy, inclusive, sustainable, innovative and secure growth and by promoting the acceleration of the process of the regional economic integration.

The topic of interest is the recognition of the necessity and importance of protecting privacy and information flow by the APEC economies, in particular through the APEC privacy framework. It is conceived to protect privacy within and beyond economies and to allow secure regional transfers of personal information benefits consumers, businesses, and governments.

This framework, as it will be further analysed, is used as a basis for the APEC Cross-Border Privacy Rules (CBPR) System.[109]

3.2.1. The Council of Europe Legal Framework

The Members of the Council of Europe have agreed, in 1950, to the Convention for the Protection of Human Rights and Fundamental Freedoms, with the aim to guarantee an effective recognition and protection of those rights necessary for the achievement of justice and peace throughout the countries.[110]

Relevant for the scope of this research is an overview on Article 8 of the Convention, within the interpretation given by the European Court of Human Rights ("ECtHR"), whose primary scope is the protection against public authority arbitrary interferences with the family life, home or correspondence of individuals.

Although the Article does not refer explicitly to data protection, the ECtHR in its case law has recognized that from the rights protected by that provision could derive the right to privacy and the right to personal data protection.[111] In its works it has been dealing with a huge variety of cases regarding different aspects of the right to privacy and of the protection of personal data.

---

[109] Asia-Pacific Economic Cooperation, https://www.apec.org/About-Us/About-APEC.

[110] Council of Europe, Preamble to the Convention for the protection of Human Rights and Fundamental Freedoms.

[111] I-Ching Chen, *Government Internet Censorship Measures and International Law*, (Wien, Zweigniederlassung Zurich: LIT VERLAG GmbH & Co. KG, 2018).

For example, regarding the topic of the disclosure of personal data, an emblematic judgment is "Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland" of 2017. In this case, after two companies had shared the personal tax information of 1.2 million people, the domestic authorities complained that such wholesale disclosure of personal data had been unlawful under data protection laws, and had forbidden such types of publication for the future too. The companies responded that the ban, instead, had violated the fundamental right to freedom of expression.

The Grand Chamber of the ECtHR stated that there had been no violation of Article 10 of the Convention (which promotes the right to freedom of expression), even if it noticed that the ban had interfered with the companies' freedom of expression.

The decision of the Chamber was upheld on the fact that the ban did not violated the Convention because it was pursuant to the law, its aim of protecting individuals' privacy was a legitimate one, and there was a perfect balance between the right to privacy and the right to freedom of expression.

Thus, the Grand Chamber agreed with the decision of the domestic courts, affirming that the mass collection and wholesale dissemination of tax data could not be justified under the scope of public interest, nor under the one of the journalistic aim.[112]

In the context of the Storage and use of personal data, instead, an interesting case is "S. and Marper v. the United Kingdom", in which the Grand Chamber stated that "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention."

Furthermore, it asserted that domestic law must guarantee the proper safeguards to the use of personal data, which has to be consistent with the Article 8 of the Convention. The Grand Chamber expressed itself also in the light of the opportunity to collect data, stressing the fact that they have to be used only in relation to the purposes for which they are stored and only during the period strictly required to carry on those purposes.[113]

---

[112] European Court of Human Rights, *Personal data protection, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, Factsheet – Personal data protection, Press Unit, October 2020, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf , (accessed 08 January, 2021).

[113] European Court of Human Rights, *Personal data protection, S. and Marper v. the United Kingdom* Personal data protection, Press Unit, October 2020, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf , (accessed 08 January, 2021).

Another case in which the Court recognized the protection of personal information under the meaning of article 8 of the ECHR is *Von Hannover v. Germany.* In this case, the Monegasque princess contested the publication of photographs displaying moments of her private life, even if those photos had been taken in public places. According to the applicant, the German Courts did not promote her rights effectively.

The ECtHR stated that despite the activities, during which the person has been immortalized, taking place in public places, "a zone of interaction of a person with others, even in a public context, fall in the scope of private life". In that occasion, the Court also recognized that with the development of new technologies, which allow efficient and quick reproduction and storage of personal data, a further and deeper protection of private human sphere was necessary.[114]

In the case *Leander v. Sweden,* the ECtHR declared the right to access personal information by their owners, held by public authorities. The case was about the dismissal of the applicant, due to national security concerns, from the Swedish Naval Base. The reasons provided for the dismissal were on the basis of personal files, to which access was denied by the employer.

The Court analysed the link with private life of the employee and declared that: "It is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8.1".[115]

This openness through the "private life" notion is justified by the fact that there is not a universal and comprehensive definition of it, but it comprises numerous interests regarding the private sphere of an individual, such as correspondence (traditional and technological ones), home and family life and communication.

The concept of private life changes constantly along with the needs of the society, for example, it also relates to a person's image, and the right the individual has on photographs and video-clips featuring her/him. It also affects peoples' personal growth

[114] European Court of Human Rights, "Von Hannover v. Germany", *Application No. 59320/00*, June 24, 2004): para. 50 – 70.
[115] European Court of Human Rights, "Leander v. Sweden", *Application No. 9248/81*, Series A no. 116, March 23, 1987): paras. 9-16, 48.

and identity and concerns the field of human relationships. The family environment is not the only one covered: business and professional activities are also included.[116]

The ECtHR reaffirmed its position also in more recent decisions. An example can be found in the case *Ben Faiza v. France*, which concerned surveillance measures taken against the applicant during an investigation about his responsibility in drug-trafficking offences. The applicant declared that the measures relating to the installation of a geolocation device on his vehicle along with the French Court order, issued to a mobile telephone operator, to obtain records of his calls, resulted in an interference with his right to respect for his private life.

According to the ECtHR, there had been a violation of Article 8 of the Convention caused by the real-time geolocation of the applicant's vehicle by means of a GPS device on 3 June 2010, finding that, in the field of geolocation measures, French law did not indicate with enough clarity to what extent and how the authorities could use their discretionary powers. Thus, it had not been ensured to the applicant, the minimum protection guaranteed by the rule of law in a democratic society. Subsequently, France had adopted a legislative mechanism ruling about geolocation use, which promoted the right to respect for privacy.

For this reason, the Court further stated that there had been no violation of Article 8 concerning the court order issued to a mobile telephone operator on 24 July 2009 to have the access to the list of cell towers pinged by the applicant's mobile device for following his movements. It then noticed that the French Court order had resulted in an interference with the applicant's private life. Notwithstanding that, it was in accordance with the law. Moreover, the order had been aimed at solving a case concerning criminal proceedings for the importing of drugs, criminal conspiracy and money laundering, and so the French Court had pursued the legitimate aims of preventing disorder or crime and of protecting public order and health. The European Court of Human Rights defined those measures as "necessary" in a democratic society because aimed at breaking up a major drug-trafficking operation. Lastly, the information collected by the French Court had been

[116] *Ibid.*

used in an investigation and a criminal trial during which the applicant had been guaranteed an effective review and right to defence, perfectly consistent with the law.[117]

A very recent case, examined by the ECtHR is "Gaughran v. the United Kingdom" of February 2020. The topic of this case is one of the issues more recalled in this research, which is the upkeeping of personal data even after having exhausted the scope for which they were collected. More precisely, the application concerned a complaint about the indefinite holding of personal data (in the specific case they consisted of DNA profile, fingerprints and photograph) of a man who had a spent conviction for having driven under the effect of alcohol in Northern Ireland.

The ECtHR stated that there had been a violation of Article 8 of the Convention, and in particular it held that the United Kingdom had gone beyond the acceptable margin of appreciation and that the undefined time of retention resulted in an excessive interference with the applicant's right to his private life.

The Court stressed also that it was the absence of any guarantees to be decisive for its conclusion. Indeed, the personal data of the applicant had been retained indefinitely without taking into account the seriousness of his offence and without any possibility of review.

In its judgment the Court concluded that the undefined holding of the applicant's data had failed to find a fair balance between the competing public and private interests.[118]

As mentioned above, the Member States of the Council of Europe in 1981 have agreed to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

It came into force on 1 October 1985 and follows the aim of the Council of Europe to strengthen the unity of its members, respecting the principles of law, according to human rights and fundamental freedoms.[119]

It is interesting to examine the Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which is an

[117] European Court of Human Rights, *Ben Faiza v. France, ECHR 050 (2018.)*

[118] European Court of Human Rights, *Gaughran v. the United Kingdom,* February 13, 2020.

[119] Council of Europe, Preamble of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

instrument, provided by the Committee of Ministers of the Council of Europe, with the aim to simplify the understanding of the Convention's provisions.[120]

The idea of adopting a Convention concerning the protection of personal data came from the identification of the need of new legal rules to govern the increasing use of automated means for public and administrative scopes. Indeed, computer's storages give the possibility to retain and to process larger quantitative of information, in comparison with manual files. Consequently, the Council of Europe felt urge the need of a more complete legislation also to let individuals exercise control over data concerning themselves.

This need had been strengthened by the fact that from a study carried out by the Committee of Ministers came up that the national legislations, in force at that time, were not able to guarantee a sufficient level of privacy protection to data retained in automated data servers.

Thus, the Committee of Ministers adopted in 1973 and 1974 two resolutions dealing with the storage of personal data in electronic data base. Some issues arose regarding the transborder flows of personal data, on the ground that developments in technology and telecommunications allowed processing of data at international level, and the standard of protection ensured was not the same in all the countries.

Differences in data protection rate could lead to the behaviour of data users, which, to avoid strict controls of data protection, transfer their operations on data to countries with low or inexistent data protection rules and controls, the so-called "data heavens".

To avoid these unfair practices, some countries replied with the establishment in domestic law of special controls, such as the license for export: these types of controls may negatively impact the free flow of information across countries, a fundamental principle for both countries and individuals.

Also for this reason, it became of primary importance for the Council of Europe to find a solution for preserving this principle.

[120] Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *European Treaty Series – No. 108,* Strasbourg, 28.l.1981.

During the drafting process of the resolutions on data protection, the Committee of Experts stressed the necessity of reinforcing those rules through the adoption of binding agreements at international level.

The result was the elaboration of two models: one based on the principle of reciprocity, according to which a country could impede the performance of data operations related to individuals from other countries if those activities did not respect the law of the first country; the other one, instead, was oriented through the establishment of the same data protection principles for all Parties. The latter was preferred by the Committee of Ministers, due to the fact that the first model assumed that peoples did not enjoy the same rights. Consequently, a Committee of Experts on Data Processing was established,[121] with the aim "to prepare a convention for the protection of privacy in relation to data processing abroad and transfrontier data processing".[122]

The Committee collaborated with the Organisation for Economic Co-operation and Development (OECD) and also with non-European countries. The final text was approved by the European Committee on Legal Co-operation (CDCJ) and the Committee of Minister opened it for members approval on 28 January 1981.

The main principle upon which the Convention was built was that some individual's rights had to be protected hand to hand with the regime of free flow of data across boundaries, according with Article 10 of the ECHR - as it states that "to receive and impart information and ideas without interference by public authority and regardless of frontiers" - and with Article 19 of the International Covenant on Civil and Political Rights, which guarantees the right to "receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice".

More specifically, in its wording it lays down principles concerning the use and the processing of personal data by the contracting parties.[123]

"Article 1 – Object and purpose

[121] *Ibid.*

[122] Activity No. 21.20.1 of the Programme of Intergovernmental Activities.

[123] Council of Europe, Preamble of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").[124]"

The first Article of the Convention underlines the link between the right to privacy and personal data protection.[125] All the activities carried out on the internet involve the automatic processing of personal information: E-mails, social networks, research via browsers led to a dissemination of data on the web.

In this context, Convention 108 has the purpose to protect individuals, whatever his/her nationality or residence, from the improper treatment of personal information.

Through the principles stated in the Convention, the emphasis is given to the processing lawfulness and the user's consent. Convention 108 contains a series of rules addressed to private companies and public authorities. In particular, the user has to be informed on all the activities, which involve her/his personal data, and has to give explicit consent upon those operations.[126]

The Convention also provides that the storage of data has to be legitimate and it is also stated that the period of retention should not be unlimited, but it has to be defined the bare minimum to carry out the entitled purposes, recognising the necessity of combining the protection of the fundamental values of the respect of privacy with the free flow of information between peoples.[127]

Indeed, the Convention could be ratified also by non-member states of the Council of Europe and extra EU countries. Currently, the Convention has been ratified by all the 47 Member States of the Council of Europe, and by Mauritius, Senegal, Uruguay and Tunisia. [128]

---

[124] Convention 108, Article 1: "The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

[125] *Ibid.*

[126] European Union Agency for Fundamental Rights, *Handbook on European data protection law,* (Luxemburg: Publication Office of the European Union, 2014): 11-31.

[127] *Ibid.*

[128] Council of Europe Portal, *Convention 108 and Protocols,* https://www.coe.int/en/web/data-protection/convention108-and-protocol (accessed March 10, 2020).

In the next paragraph, we will see to what extent this Convention has influenced EU law concerning data protection and the right to privacy.

In conclusion, the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data of the Council of Europe deserve a mention.

These Guidelines, concerning the protection of personal data, have been issued on January 2017 and their scope is to suggest the measures that Parties, controllers and/or processors should implement to avoid negative impacts of the use of Big Data on people, to preserve human rights and fundamental individual and collective freedoms.

In particular, Big Data operates in the society providing opportunities for innovation, increasing productivity and promoting social participation. What the Guidelines are interested at is the process of personal data involved in Big Data. They are conceived to support policy makers in the protection of the processing of such data, to preserve people fundamental rights and to place them at the centre of digital economies.

Thus, they offer a guidance for the protection of those rights in the different fields in which Big Data are used, from the health sector to the financial one.

It has to be noted that, in the context of the evolution of digital technologies, the Guidelines may be updated in the future as deemed necessary by the Committee of Convention 108.

However, the Guidelines should not be interpreted as a limitation or a substitution of the provisions of Convention 108 and of the European Convention on Human Rights, on the contrary they have to be thought as their support and reinforcement.[129]

3.2.2 The European Union Legal Framework

The European Union has a leading position in the protection of data, revealing itself as a forerunner on the protection of individual life and private information. The entire European Union system has created a strong regime for the protection of privacy

[129] Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Consultative Committee of the convention for the protection of individuals with regard to automatic processing of personal data, (Strasbourg: January 23, 2017).

and personal data which has become a source of inspiration for the various data protection regulatory frameworks worldwide. [130]

In the European Union Legal Framework, one of the instruments providing the right to data protection was the Directive 95/46/EC, also known as the Data Protection Directive (DPD). It has been an evolution of the Convention 108 of the Council of Europe and it has put the basis for the further development of the legislation in the field of the protection of personal data, which culminated with the adoption of the GDPR, which repealed the Directive 95/46/EC.

The Directive, regarded as the main legal instrument on data protection, was established with the main purpose of harmonizing the legislative framework of the EU Member States to guarantee a high and unified standard of protection of personal data.[131] As the CJEU stated "Directive 95/46 is intended […] to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. […] The approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the EU. Accordingly, […] the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete."[132]

The Data Protection Directive was applicable not only to Member States, but also to non-EU Member States part of the European Economic Area (EEA)[133], as Iceland, Liechtenstein and Norway. The control of the compliance and the fulfilment of the Member States obligations was under the jurisdiction of the Court of Justice of the European Union (CJEU).

The Data Protection Directive gave a quite precise definition of personal data: "(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or

---

[130] European Union Agency for Fundamental Rights, *Handbook on European data protection law,* (Luxemburg: Publication Office of the European Union, 2014).

[131] European Union Agency for Fundamental Rights, *Handbook on European data protection law,* (Luxemburg, Publication Office of the European Union, 2014): pp. 11-31.

[132] Court of Justice of the European Union, "Joined cases C-468/10 and C-469/10", *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, November 24, 2011: paras. 28-29.

[133] Agreement on the European Economic Area, OJ 1994 L 1.

indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"[134].

Article 3, instead, was about the scope of the Directive. It clarified that the application of the DPD did not involve either the activities not the object of Community law, neither the operations conducted by a natural person during the performance of a personal or household activity.[135]

A necessary element for the legitimacy to carry out operations on personal data was the "consent". It had to be given both in an explicit or an implicit way and it had to result from the circumstances in an unambiguous way.[136]

Other relevant provisions of the Directive were those concerning fairness and lawfulness of the processes, legitimacy and explicitness of the collection of data. It continued stating that information had to be kept only as long as they serve to the scope, and it had to be recognized to the owner the right to update such information. About the transparency of the operations, as soon as there was the suspect of the inaccurateness or the incompleteness of information, all the means had to be ensured for the control or rectification of the inadequacies. The Directive also provided the possibility to keep some data for longer periods when this was required by historical, scientific, or medical use, but it prescribed to the Member States the supervision on the justifications for the protraction of the storage.[137]

According to Chapter II of the Directive, the management of personal data had to be conducted in compliance with the principles of the Directive listed in article 6 and with at least one of the requisites of Article 7.[138]

This means that operations on personal data could had been carried on only if (a) the owner of the information had given his consent in an unambiguous way; or if (b) the processing was necessary for the performance of a contract to which the data subject was

---

[134] Data Protective Directive, 95/46/EC, Article 2 (a).

[135] Data Protective Directive, 95/46/EC, Article 3 (2).

[136] Data Protective Directive, 95/46/EC, Article 7: "(a) the data subject has unambiguously given his consent"; Data Protective Directive, Article 26: "(a) the data subject has given his consent unambiguously to the proposed transfer".

[137] Data Protective Directive, 95/46/EC, Article 6.

[138] European Court of Justice, "Heinz Huber v. Bundesrepublik Deutschland*", cases C-542/06,* December 16, 2008): para. 48; European Court of Justice, "Asociacion Nacional de Establecimientos Financiarios de Crédito and Federacion de Comercio Electronico y Marketing Directo v. Administracion del Estado" *Joined cases C-468/10 and C-469/10,* November 24, 2011): para. 26.

party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing was necessary for compliance with a legal obligation to which the controller was subject; or (d) processing was necessary in order to protect the vital interests of the data subject; or (e) processing was necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing was necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data were disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."[139].

In any case, these stakes might not be in contrast with fundamental rights and freedoms of the data owner. Even States could not add new requirements or principles regarding the operations on personal data with the scope of overriding the principles stated in Article 7, where the list of cases in which the operation on personal information could had been considered lawful was regarded as complete by the European Court of Justice.[140]

The Directive ruled also about the processing of sensitive data. Here the legislative protection was extended: for example, the explicit consent of the data subject was required, the interest of the data subject had to be essential and legitimate.

Other principles guaranteed by the DPD included the transparency of data processing. Controllers were entitled to fulfil specific obligations regarding notification and publication. Their duty was to inform the competent supervisory authority about the operations conducted for future publication of notifications in the form of a register.[141] Each Member State had to establish an institutional structure with the function of an independent supervisory or oversight body with various tasks like investigation and intervention. Also, the power to establish legal proceedings and the possibility to hear complaints are its most important duties.[142]

---

[139] Data Protective Directive, 95/46/EC, Article 7 (a)-(f).

[140] European Court of Justice, "Asociacion Nacional de Establecimientos Financieros de Credito and Federacion de Comercio Electronico y Marketing Directo v. Administracion del Estado", *joined cases C-468/10 and C-469/10*, November 24, 2011: para. 30, 32.

[141] Data Protective Directive, 95/46/EC, Article 18, 19, and 20.

[142] Data Protective Directive, 95/46/EC, Article 28.

According to the principle of fair processing, data owners had the right to be informed of any action brought on their personal information and also of the identity of the subject who carries on those actions, so the controller. Specifically, there should be clarified the processing purpose and the period in which the data would be held.[143]

The DPD provided the establishment of another institutional structure: the so-called "Article 29 Working Party on the Protection of Individuals about the Proceeding of individual information", made of authorities or representatives of the supervisory authority and entitled of advisory functions.[144] Exemptions were provided in cases data were collected for statistical purposes or for approved studying researches, if the recording or the acquisition of such information would be of a disproportionate effort. [145]

There were other derogations for the collection and/or the disclosure of data expressly guaranteed by the law,[146] for example it could have been required by national issues, such as in terms of public security, or to avoid criminal offences, to safeguard crucial economic or financial interests of the States and to promote the most important rights and freedoms of the data subjects.[147]

To satisfy the need of a stronger data protection legal framework, the European Commission published the proposal for its final data protection framework on 25 January 2012, the General Data Protection Regulation (GDPR).[148], entered into force in 25 May 2018 in all member States and it has the purpose to harmonize data privacy laws across Europe.[149]

It comprises various amendments to the legal framework contained in the DPD, as its main purpose was elevating the standards of data protection to ensure a better and comprehensive protection of individuals' rights and to establish a coherent framework involving all areas of competence of the European Union.[150]

---

[143] Data Protective Directive, 95/46/EC, Article 10 (a)-(c).
[144] Data Protective Directive, 95/46/EC, Article 29 and Article 30.
[145] Data Protective Directive, 95/46/EC, Article 11 (2).
[146] *Ibid.*
[147] Data Protective Directive, 95/46/EC, Article 13 (1).
[148] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", *COM(2012) 11 final*, January 25, 2012.
[149] Intersoft Consulting, "General Data Protection Regulation, GDPR", available at https://gdpr-info.eu (accessed August 2020).
[150] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such

The first relevant difference is that, from a formal perspective, the GDPR is a Regulation and, as stated in Article 288 of the Treaty on the Function of the European Union (TFEU), it is directly applicable in all Member States, resulting in a higher level of harmonization than the one ensured by the Directive. This difference has been considered favourably because it can solve some competences problems and because it would let the adequacy of privacy standards be an issue at EU level.

At substantial level, important amendments refer to the right to deletion of collected data, data minimization, the implementation of surveillance principle, the formal inclusion of the right to be forgotten, etc.[151]

For the scope of this research, it is relevant to address which cases the Regulation applies to and whose are the beneficiaries of the Regulation.

Article 2 of the GDPR, under the heading "Material Scope" states that "the Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".[152]

This means that any type of conducted process of personal data falls within the scope of the GDPR. This provision has been interpreted in a broad way that covers all the companies' operations on data, so as to be able to ensure extremely high protection levels.[153]

The beneficiaries of the GDPR are all the individuals, without distinction of nationality or state of residence. [154] Stronger protection is ensured to minors, which, due to their vulnerability and their lower awareness of their rights, are more exposed to all risks regarding the processing of personal information.[155]

However, a category which does not benefit from the protection under the GDPR is the one of legal persons, and in particular undertakings established as legal persons.[156]

---

data*",* General Data Protection Regulation, 25.1.2012, COM (2012) 11 final, 2012/2011 (COD) January 25, 2012: p. 4.

[151] Rolf H. Weber*,* "Transborder data transfer: concepts, regulatory approaches and new legislative initiatives", *International Data Privacy Law*, Vol. 3, Issue 2, May 2013: pp. 117-130.

[152] General Data Protection Regulation, Article 2.

[153] Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR), A Practical Guide,* (Germany, Hamburg: Springer International Publishing AG 2017).

[154] General Data Protection Regulation, Rec. 14.

[155] General Data Protection Regulation, Rec. 38.

[156] Data Protection Directive, Rec. 14.

Only if the data contains information of individuals linked to the legal person, they could fall under the scope of the GDPR: this is the case, for example, of data regarding the information on a persons' share in a company.[157] An exception, instead, is provided for one-person-owned entities: this is deemed as a natural person, because in such a situation it is not possible to distinguish between personal and corporate data.[158]

The GDPR also defines the territorial scope of its norms. Article 3 of the Regulation states that it applies to personal data operations conducted by a controller or/and a processor in the Union, irrespective of whether activities take place in the EU territory. Moreover, it covers operations on information related to European data subjects conducted by controllers or/and processors that are not established in the EU territory, when the activities concern: "(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of the behaviour as far as their behaviour takes place within the Union".[159]

The last paragraph of the article relates to the operations on personal data conducted by controllers established in a non-European territory where the law of a Member State applies by virtue of international law: in these cases, the GDPR applies too.[160]

Although to this extent the territorial scope of the GDPR goes beyond the EU boundaries, it had been justified by the phenomenon of globalization, which affects also the global economy, especially through the activities of multinational groups and enterprises and the huge amount of cross-border data transfers worldwide.

The Regulation brings also the establishment of a new body, the European Data Protection Board that has to replace the Article 29 Working Party mentioned above. The innovation consists of the institution of heads of the supervisory authority of each Member State and of the European Data Protection Supervisor.[161]

As anticipated above, one of the main innovations coming from the GDPR legal regime is the one referred to the so called "right to be forgotten".

---

[157] Stefan Ernst, in Boris P. Paal, Daniel A. Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetx*, Beck'sche Kompakt-Kommentare, (München: Verlag C. H. Beck oHGArt, 2018).

[158] Peter Blume, "The data Subject", *European Data Protection Law Review,* 2015: 258, 258.

[159] General Data Protection Regulation, Article 3.

[160] General Data Protection Regulation, Article 3.3.

[161] General Data Protection Regulation, Article 64.

In particular, it is a concept which had been introduced by the Court of Justice of the European Union (CJEU) in the context of the judgment *Google vs. Spain*[162] on 13 May 2014[163], in which the CJEU stressed that, according to the Directive 95/46/EC, Google should have delated from its search engine the links containing information related to the requester, on the basis that Internet search engine operators are responsible for all the performances involving private information which appear on the web. The CJEU introduced this new expression on the basis of individuals right promoted by Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union, respectively: the respect for private and family life and the protection of personal data.[164]

This judgment brought a significant innovation also in the context of the draft and for interpretation of the GDPR.

Indeed, the "right to be forgotten" had to be included as such in the Regulation, but in the final version it had been changed in favour of the right to Data Erasure, which guarantees the right of the data subject to have her/his personal data erased by the controller under certain circumstances.

This provision applies when the data "are no longer necessary in relation to the purposes for which they were collected or otherwise processed"; when "the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing"; when "the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the

---

[162] European Court of Justice, "Google Spain, C-131/12", ruling of May 13, 2014:
"1. This request for a preliminary ruling concerns the interpretation of Article 2(b) and (d), Article 4(1)(a) and (c), Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 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 (OJ 1995 L 281, p. 31) and of Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter'). 2. The request has been made in proceedings between, on the one hand, Google Spain SL ('Google Spain') and Google Inc. and, on the other, the Agencia Española de Protección de Datos (Spanish Data Protection Agency; 'the AEPD') and Mr Costeja González concerning a decision by the AEPD upholding the complaint lodged by Mr Costeja González against those two companies and ordering Google Inc. to adopt the measures necessary to withdraw personal data relating to Mr Costeja González from its index and to prevent access to the data in the future."

[163] Noam Tirosh, "Reconsidering the "Right to be Forgotten" – memory rights and the right to memory in the new media era", *Media, Culture and Society,* Vol 39, no 5, (2017): 644–660.

[164] Robert C. Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere," *Duke Law Journal* Vol 67, no. 5 (February 2018): 981-1072.

processing pursuant to Article 21(2)"; if "the personal data have been unlawfully processed"; or in case "personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject"; and/or if the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."[165]

Also here are provided exceptions in case data processing has to be conducted in order to comply the right to freedom of expression and information, when there are legal obligations that need to be satisfied and when other interests such as public issues, scientific or historical purposes come up.[166]

At paragraph 2 of Article 17, it is recognized the right of the data subject to ask the controller, to publish her/his request of deleting the personal information held, so that, by making public that request, all the holders of the personal data may accomplish to the deletion demanded.[167]

However, the principle issued in Article 17 of the GDPR has been subjected to some critics. If it is true that the article is a means by which the data subjects can compel controllers to erase their personal information, at the same time it is acknowledged that the work of controllers and processors with the uncontrolled development of technology has become more and more a challenge. Indeed, it is everyday more difficult in terms of costs and advanced technologies to ensure a complete deletion of all information detained, since computers and software are increasingly improved with the precise purpose to hold tight the information they get.[168]

---

[165] *Ibid.,* Article 17.

[166] *Ibid.,* Article 17.3(c); Article 17.4(d).

[167] General Data Protection Regulation, Article 17 (2): "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data."

[168] Gehan Gunasekara, "Paddling in Unison or Just Paddling? International Trends in Reforming Information Privacy Law*", International Journal of Law and Technology*, Vol. 22, No.2, 2014: 141-177; Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in David Wright and Paul De Hert, *Privacy Impact Assessment,* (Dordrecht Heidelberg London New York: Springer 2012): 33-59.

Further analysis of the GDPR will be proposed in the second and the third chapters of this thesis, especially with reference to the legal discipline of cross border data flows and possible restrictions on them.

As anticipated above, with the Charter of Fundamental Rights of the EU ("CFR"), data protection and the right to privacy have been elevated to the status of fundamental human rights.

As already mentioned above, Article 8 of the Charter states that:

> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. Compliance with these rules shall be subject to control by an independent authority.

Article 8 of the Charter has been based on Article 286 of the Treaty establishing the European Community – now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union - and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

According to Article 8 of the Charter[169], which is considered one of the most open-ended provisions of the Charter, the requisites for the processing and the use of personal information are the transparency and the legitimation.

[169] European Charter of Fundamental Rights, Article 8 - Protection of personal data: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her,

To meet the first requisite, the consent of the user operating with its data is needed. Furthermore, the owners of information should have free access to their data alongside the possibility to recover it. Legitimation means that everything should be collected for a specific and justified purpose.

Among the most relevant cases concerning the application of the Article 8 of the Charter, it would be interesting to look at one of the latest judgments of the CJEU on the topic, which is "Case C-136/17/ (GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)".

In particular, it consists of a request for a preliminary ruling with the object of the interpretation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals in relation to the processing of personal data and the free movement of such data by a search engine. In this context the Court ruled that the provisions of Article 8(1) and (5) of Directive 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 provide that the prohibition or limitations to the processing of special categories of personal data, apply to the operator of a search engine because the protection of personal data is a fundamental principle and it falls within the context of his responsibilities, powers and capabilities.

The provisions of Article 8(1) and (5) of Directive 95/46 must be interpreted as meaning that the operator of a search engine is in principle required by those provisions, subject to the exceptions provided for by the directive, to accede to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions.

More specifically the Court stated that the provisions of Directive 95/46 must be read as meaning that, where the operator of a search engine has received a claim for the elimination of a personal reference from a web page, the operator must, taking into account the relevant factors of the particular case and having regard to the seriousness of the interference with the data subject's fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the

---

and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."

European Union, determine, having regard to the possible issues of public interest referred to in Article 8(4) of the directive, whether the inclusion of that reference is necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter, otherwise the right to protection of personal data prevails.[170]

Other relevant judgments of the EUCJ are the one referred to the Case C-623/17, Privacy International, and the Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others, in which the Court of Justice confirmed that under EU law national legislation requiring a provider of electronic communications services is precluded to carry out the global and indiscriminate transfer or retention of traffic data and location data for the purpose of combating crime both for general and for safeguarding national security.

The Court specified that the directive on privacy and electronic communications, has to be interpreted in the light of the principle of effectiveness, which prescribes to national criminal courts the disregard of information and evidence acquired by means of the general and indiscriminate holding of data in breach of EU law, in the context of such criminal proceedings, where people suspected of having committed a crime are not in a position of advantage to express themselves on that information and evidence.[171]

In conclusion, also some Regulation and Directives of the EU can be listed among the EU legal instruments concerning data protection.

In particular, the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, defines the processing of personal data, affirming that Processing of personal data pursuant to the Directive shall be carried out in accordance with Directive 95/46/EC, and that processing of personal data by Union

[170] European Union Agency for Fundamental Rights, *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL),* CJEU Case C-136/17/ Judgment, https://fra.europa.eu/en/caselaw-reference/cjeu-case-c-13617-judgment (accessed January 08, 2021).

[171] Court of Justice of the European Union, *Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others*, and C-520/18, Ordre des barreaux francophones et germanophone and Others, Luxembourg, 6 October 2020.

institutions and bodies pursuant to the Directive shall be carried out in accordance with Regulation (EC) No 45/2001.[172]

Then, the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA should be mentioned.

It addresses to Member States for the protection of fundamental rights and freedoms of natural persons and in particular for their right to the protection of personal data. Article 4 of the Directive enhances the principles relating to processing of personal data.

It reaffirms the principles set out in the international sources of law and in particular, it refers to Member States which have to ensure the lawful and fair processing of personal data; the specified, explicit and legitimate purpose of the collection of information; the proportional use of those data to the purposes for which they are processed; the accuracy of data, which have to be kept up on date, ensuring all the necessary instruments to rectify and modify data which are not reliable anymore; the keeping of data in a form which permits identification of data subjects for the time necessary for the purposes for which they are collected and processed; the protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.[173]

Moreover, the Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, in relation to the protection of personal data states that "Each Member State shall

[172] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Article 2.

[173] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Article 4.

provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to protection of their personal data, rights of access, rectification, erasure and restriction and rights to compensation and judicial redress as laid down in Union and national law and in implementation of Articles 17, 18, 19 and 20 of Framework Decision 2008/977/JHA (*supra*)."[174]

Another relevant legal instrument can be identified in the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

The provisions of interest are the Article 5 and Article 6. The latter rules about the illegal interception, condemning the illegal collection and use of data.[175] Article 5, instead, rules about the illegal data interference referring to Member States which "shall take the necessary measures to ensure that deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor".[176]

Among the Regulations of the EU, the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC lays down provisions for the protection of people, regarding the processing and the free movement of their personal data. At paragraph 2 of Article 1 it explicitly held the protection of personal data as a fundamental right and freedom of natural persons.[177]

Finally, the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), also rules about personal data and states the general principles

[174] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Article 13.
[175] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Article 6.
[176] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Article 5.
[177] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Article 1.

about data protection, reminding the Directive (EU) 2016/680, which has been analysed above in this paragraph. It refers for example to the processing of personal data which has to be fair and in compliance with laws and legislations; to the collection of data which has to be justified and limited in time having regard to the purposes for which they are processed, etc.[178]

3.2.3 The Organization for Economic Co-Operation and Development (OECD) Legal Framework

The Organization for Economic Co-Operation and Development (OECD) is an international organization composed of thirty-six nations, which works mainly as a consultative assembly to compare political experiences, for the resolution of common problems, the identification of commercial practices and the coordination of local and international policies of the member countries regarding prosperity, equality, opportunity and well-being[179].

It was conceived by 18 European countries, Canada and the United States and established in 1960 with the aim of encouraging development and economic growth. The purpose of the Organization lies in the promotion of policies to increase human beings' standards of living. [180]

Regarding data protection, OECD has an effective policy both inside the Organization – as OECD staff is obliged to conduct its tasks in a transparent and appropriate way to guarantee the protection of the personal data managed [181]- and outside the Organization, influencing Member States' behaviours.

The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data play a prominent role at international level regarding the legitimacy of the system.[182] In the Part Two of the Guidelines, eight principles are stated that should to be applied by the Governments, some of them indicating the methods for the collection of data, their retention and maintenance.

---

[178] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), Art. 28.
[179] OECD, "Who we are", https://www.oecd.org/about/
[180] OECD, "Better Policies for Better Lives", http://www.oecd.org/about/. (accessed March 15, 2020).
[181] *Ibid.*
[182] *Ibid.*

Moreover, those instructions are provided for the fair circulation of data to ensure that information are not spread or shared without justified reasons. Through the principles finds its place the one about the necessity of the consent of the individual for the fair conduction of data-related operations. Additionally, it is provided to people the right to access to their personal information and the right to claim for the possible wrongness of data detained, allowing all corrections when and where it would be necessary.

In the Guidelines there are also references to the general principles of good faith, transparency and fairness.[183]

Notwithstanding the non-binding status of those principles, they exercise a strong influence across the national and international legislations for the promotion and the protection of information privacy, and therefore they are considered guiding rules, especially in accompanying the evolution of data protection.[184]

To strengthen the level of protection, it is necessary to update these principles, to make them closer to the needs of defence coming from the advancing of new technologies: modern communications networks contribute to the changes of society, and legislations have to find themselves ready to face the new developments.

For this reason, OECD periodically publishes updated Guidelines.[185] They have encountered great success among Member States and on the whole international community.[186] Evidence can be found in the Asia-Pacific Economic Cooperation Privacy Framework, European Unions' Privacy Directive and in the US-EU "Safe Harbor" regime.

3.2.4 The Asia-Pacific Economic Cooperation (APEC) Legal Framework

[183] Wafa Tim, "Global Internet Privacy Rights – A Pragmatic Approach*", University of San Francisco Intellectual Property Law Bulletin*, Vol. 13, May 31, 2009: 131-159.

[184] Peter Blume, Peter Seipel, Ahti Saarenpää, Dag Wiese Schartum, *Nordic Data Protection*, (Iustus Förlag, Uppsala 2001): 6.

[185] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.

[186] OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_ framework.pdf, (accessed March 20, 2020).

For completeness in presenting the regional legal framework which governs the protection of personal data, it is necessary to introduce the Asia-Pacific Economic Cooperation privacy framework.

The Asia-Pacific Economic Cooperation (APEC) is an inter-governmental forum established in 1989, which comprises 21 member economies in the Pacific Rim, and it promotes the liberalization of trade throughout the Asia-Pacific region.[187]

APEC member economies realized the potential of electronic commerce to increase business opportunities, lower the costs, improve efficiency, increase the quality of life, and simplify the participation of small business in global affairs. For these reasons, a framework to enable regional data transfers benefiting consumers, businesses, and governments was chosen: this was the APEC Privacy Framework. It was endorsed by Ministers which recognized the importance of the development of effective privacy protections that remove barriers to information flows, ensure continued trade, and economic growth in the whole APEC region.[188]

For the purposes of the present analysis, it should be highlighted that in 2005 the parties to the forum agreed on the APEC Privacy Framework, which promotes a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.[189].

The purpose of the Framework is to regulate economic transactions, in order to ensure consumer trust and to avoid the exploitation of electronic commerce in favour of the economies. Sharing benefits between consumers and economies is one of the main reasons for the adoption of the Framework, as stated into its Preamble.[190]

The APEC Framework is used as a basis for the APEC Cross-Border Privacy Rules (CBPR) System, which is conceived to ensure a coherent policy for privacy and personal information protection in the Asia-Pacific region, and to promote regional integration and economic growth.[191]

---

[187] Asia-Pacific Economic Cooperation, *APEC Privacy Framework,* APEC Secretariat, Singapore 2005.
[188] APEC Privacy Framework, Preamble.
[189] Asia-Pacific Economic Cooperation, *APEC Privacy Framework,* APEC Secretariat, Singapore 2005.
[190] *Ibid.*
[191] Discussion Draft, "Benefits of the APEC Cross-Border Privacy Rules, Protecting Information. Driving Growth. Enabling Innovation*",* https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf (accessed March 20, 2020).

The APEC Privacy Framework is composed of nine principles, similar to the UN and OECD Guidelines. These principles refer to personal information processed by personal information controller.

In particular, "Personal information" is defined in Paragraph 9 of the Framework as any information related to an identified or identifiable individual[192]; instead, at Paragraph 10, "controller" is defined as a person or an organization in charge of survey and monitor the collection, the holding and the processing of personal data[193]

APEC principles do not intend to restrict data transfers, on the contrary they are conceived to achieve economic development and strengthen cooperation among its members, being consistent with the main forum's mission of inclusion among region's populations and the achievement of high standards of living for all the actors involved. According to its policy, APEC supported the principle of accountability in compliance with modern business practices.[194]

An interesting feature of the Framework is its flexibility, proved by the fact that it can be applied in the most fitting ways to the different social, cultural and political environment. Also considering other factors such as public safety, national security or more in general, public policies, it can operate according to the actual needs.[195]

From another point of view, both its self-regulated interpretative system and its flexibility let the Members have a quite free and independent conduct, favouring their own interests, stressed by the fact that the Framework is not binding for the Member States and it does not require any oversight mechanism. The reason of this strong openness, ensured through the members' initiative and self-determination, lies on the various political and cultural environment in which it operates. Indeed, many APEC members are now developing their domestic law frameworks, while others, such as the Asiatic governments, are subjected to authoritarian streaks. On this basis, an imposition

[192] APEC Privacy Framework, paragraph 9.
[193] APEC Privacy Framework, paragraph 10.
[194] Discussion Draft, "Benefits of the APEC Cross-Border Privacy Rules, Protecting Information. Driving Growth. Enabling Innovation*",* https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf (accessed March 20, 2020).
[195] *Ibid.* paras. 9-13.

of a normative guideline would lead to objections and rejections with unpleasant consequences for the forum.[196]

In 2011, in order to ensure cross-border data privacy, the Cross-Border Privacy Rules (CBPR) System was adopted, with the approval of the 21 APEC heads of State. The system has the main aim to develop its members' economies by reviewing their policies and business rules, establishing the standards to do that. [197]

The process' system starts with the submission by organizations and/or interested actors of a self-assessment questionnaire, in which they state the recognition of an Accountability Agent within their jurisdictions. Accountability Agents are third-party organizations endorsed by APEC and their main task is the review of requesting actors' privacy policies to certify or not the compliance with CBPR system. If they result not compliant, the agents and the organizations work together to finally meet the requirements of the system. They also manage to dispute resolutions between CBPR actors and individuals. If they complete the compliance process, the requesting party is recognised as CBPR-compliant and registered on the official website. Finally, per year, they have to undertake recertification to prove that they are still CBPR-compliant. Ultimately, accountability agents have also the duty to verify if participating companies' data policies and practices are efficient to protect user data.[198]

The Framework was updated in 2015, with the introduction of concepts enhanced in the OECD Guidelines of the 2013. The Framework, which has the aim of promoting electronic commerce throughout the Asia Pacific region, has always been consistent with the core values of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines), since the first version of 2005. For this reason, in line with the publication of the OECD Guidelines of 2013, the APEC region felt the need to reaffirm the value of privacy to individuals and to the information society considering the different legal features and context of the APEC region.[199]

---

[196] Wafa Tim, "Global Internet Privacy Rights – A Pragmatic Approach"*, University of San Francisco Intellectual Property Law Bulletin*, Vol. 13, May 31, 2009: 131-159.

[197] Discussion Draft, "Benefits of the APEC Cross-Border Privacy Rules, Protecting Information. Driving Growth. Enabling Innovation*"* https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf (accessed March 24, 2020).

[198] *Ibid.*

[199] APEC Privacy Framework, 2015.

CHAPTER II - International Trade Law and Restrictions on Data Flows under WTO regime

1. International Human Rights and International Trade Law

After the Second World War, reaching peace and international order was the primary concern for many states. This led to the creation of international organizations that prioritized cooperation on economic, social, and financial policy.[200]

The aim of both structural frameworks, International Human Rights Law and International Trade Law, was to create an institutional and multilateral basis that would be able to guarantee the protection of human rights in all states, in light of increasing the overall standard of living also in terms of employment and income.

Since their foundation, human rights and international trade systems have developed significantly.

The evolution of these two systems has taken disjunctive paths and, at the same time, it presented inconsistent patterns of relation. However, in this paragraph are described the only elements which are relevant for the introduction to the topic of the protection of the right to privacy and personal data protection in the framework of the international trade law, without any claim to exhaustiveness.

From the point of view of international trade, the General Agreement on Tariffs and Trade (GATT) was ratified in 1947. Since its enactment, its policy issues have increased substantially. Originally, it dealt solely with trade tariffs, but shortly after it started to cover the field of healthcare and safety, agriculture, intellectual property, and telecommunication, areas historically been under State policy and control.

[200] Robert Howse and Makau Mutua, "Protecting Human Rights in a Global Economy: Challenges for the World Trade Organization", *International Centre for Human Rights and Democratic Development* (Leiden: Martinus Nijhoff Publishers, 2001); see also Caroline Dommen, "Safeguarding the Legitimacy of Multilateral Trading System: The Role of Human Rights Law," *in International Trade and Human Rights: Foundations and Conceptual Issues*: eds. Frederick M. Abbott, Christine Greining-Kaufmann, and Thomas Cottier, (Michigan: University of Michigan: The World Trade Forum, Vol. 5, 2006), 121-132.

In its preamble, the GATT highlights the fact that its purpose is to "rais(e) standards of living, ensur(e) full employment and a large and steadily growing volume of real income".

As a result of the Uruguay Round in 1995, the World Trade Organization (WTO) came into existence.

The objectives of the GATT preamble were reiterated in the agreement that established the WTO and particular emphasis was placed on the needs of developing countries and on the concept of "sustainable development".

For the purposes of this research, the WTO plays an important role in delivering the UN sustainable development goals (SDGs) - seventeen goals addressing a series of global challenges, such as the abolition of poverty and hunger, the accomplishment of gender equality, the improvement of industries, infrastructure and innovation, the reduction of inequalities etc. - since by referring to sustainable development in the agreement, they acknowledge the role of the organization in promoting and evaluating the respect of human rights. This indicates that trade rules and economic policies have to be consistent with human rights principles.

Nevertheless, numerous experts, as well as States, have been critical about the WTO system., since its actions strongly seem to concern the maximization of trade and not the improvement of member states living standards. The fear of many human rights advocates is that WTO rules can easily intensify free trade at the expense of vital social interests, being strongly supported by its enforcement mechanism and dispute settlement.[201]

In order to address the impact of the organization's action on marginalized groups of society, the UN Committee on Economic, Social and Cultural rights (CESCR) in 1999 proposed a motion at the World Trade Organization meeting in Seattle, Washington. They strongly suggested that the WTO needed to carry out a review of all international trade, investment policies, and rules, to analyse the consistency of treaties, legislation, and policies on trade law with those designed to protect and promote human rights.

Indeed, the UN Economic and Social Council has stated that "trade liberalization" is a means to achieve the "human well-being to which the international human rights

[201] Thomas Cottier, "Trade and Human Rights – A Relationship to Discover", *Journal of International Economic Law*, Vol.5, (2006): 121-132.

instruments give legal expression". Therefore, it must not be understood as an end, but as a mean through which a greater good can be achieved.[202]

Since international trade is one of the most relevant factors driving globalization, the rules that govern it have to be in alignment with the promotion and protection of human rights. This means that all the processes governing these rules need to be in compliance with the principles of transparency, inclusiveness, democracy, and participation, across all barriers.

Undoubtedly, the main actor in this context is the WTO. Its involvement in the redefinition, not only of governments and businesses, but also of inter-governmental organizations is paramount.[203]

2. The World Trade Organization: the historical background

The WTO is one of the younger intergovernmental organization, since it was established on January 1st, 1995.

It represents one of the most influential organizations created in the 21st century and it has been recognized as having "the potential to become a key pillar of global governance".[204]

As anticipated above, its origins date back to the General Agreement on Tariffs and Trade of 1947 (GATT 1947), which still influences WTO's functions and policy.

According to Article XVI:1 of the WTO Agreement: "Except as otherwise provided under this Agreement or the Multilateral Trade Agreements, the WTO shall be guided by the decisions, procedures and customary practices followed by the Contracting Parties to GATT 1947 and the bodies established in the framework of GATT 1947".[205]

---

[202] UN Economic and Social Council, *Statement of the UN Committee on Economic, Social and Cultural Rights to the Third Ministerial Conference of the World Trade Organization (Seattle, 30 November to 3 December 1999),* UN Doc. E/C.12/1999/9, Geneva: 26 November 1999, para. 6.

[203] Caroline M. Robb, *Can the Poor Influence Policy?* (World Bank: 1998); see also Stephan Haggard and Steven B. Webb, eds., *The World Bank Participation Sourcebook*, (World Bank: 1996).

[204] MCEJ Bronckers, "More Power to the WTO?", *Journal of International Economic Law,* 2001: 41.

[205] World Trade Organization Agreement, Art. XVI:1.

In February 1946 the United Nations Economic and Social Council established a Preparatory Committee with the purpose of writing a charter for dealing with the ambitious project of an international organization dealing with trade issues.[206]

From April to November 1947, the Committee worked in Geneva on a conference that was divided into three parts: the first part was dedicated to the task of drafting a charter for the establishment of a new institution, the International Trade Organization (ITO); the other two parts would form the General Agreement on Tariffs and Trade (GATT). Indeed, the second one was supposed to activate the creation of an effective multilateral agreement for the reciprocal reduction of tariffs on trade. Finally, the third part was devoted to writing the "general clauses" of tariff obligations.[207]

Geneva negotiations resulted into the GATT, but the ITO negotiation turned out to be more difficult. That is the reason why, even if the GATT had to perform its function along with the ITO Charter, numerous negotiators decided not to wait until the definition of the ITO Charter to bring the GATT provisions into force. Nevertheless, some problems arose for the enforcement of the GATT in national systems. In fact, in order for some countries to implement the agreement into their legal system, they had to submit it to their parliaments. Since they would have done the same for the enforcement of the ITO Charter, some countries decided not to appeal to the legislative power immediately. Rather, they decided to wait until the adoption of the ITO final draft, fearing that "to spend the political effort required to get the GATT through the legislature might jeopardise the later effort to get the ITO passed".[208]

To overcome this problem, eight countries that had negotiated the GATT 1947 decided to adopt the "Protocol of Provisional Application of the General Agreement on Tariffs and Trade" (PPA). Then, also the other fifteen countries of the original GATT 1947 contracting parties, applied the entire Parts I and III of the GATT 1947. The Part II, instead, was only applied in so far as it was not inconsistent with their legislations.[209]

Up to 1996, all the GATT 1947 provisions have been applied through the PPA.

---

[206] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).

[207] Jhon H. Jackson, *The World Trade Organization: Constitution and Jurisprudence* (London: Royal Institute of International Affairs, 1998), 15-16.

[208] *Ibid.,* 18.

[209] GATT BISD, Volume IV, 77.

Meanwhile, the ITO Charter negotiations ended in March 1948 in Havana, but it never entered into force. The reason lies in the fact that the United States decided not to approve it. As a consequence, the other participants were not interested in joining an international trade organization which would not have involved one of the world's economy leader and probably the biggest trading nation.[210]

At that point there was only a multilateral "institution" for trade: the GATT 1947. Even if it was conceived as an agreement and not an organization, it gradually assumed the scope of an institution and turned into a *de facto* international organization.[211]

The GATT 1947 attained a lot of success. It managed to noticeably reduce tariffs on trade in goods, especially in relation to those coming from developed countries. However, it did not have the same success reducing non-tariff barriers. The latter required a more elaborate institutional framework, given that negotiations on that field were more complex.

After some unsuccessful rounds of negotiations, such as the Kennedy Round and the Tokyo Round, contracting parties agreed that it was necessary to have another round of trade negotiations with a broader agenda.

They finally agreed to initiate a new Round in September 1986 at Punta del Este, Uruguay. At that point, "the World was becoming increasingly complex and interdependent, and it was becoming more and more obvious than the GATT rules were not satisfactorily providing the measure of discipline that was needed to prevent tension and damaging national activity".[212]

For these reasons, the Ministerial Declaration signed in Punta del Este was unique, since for the first time the negotiations would have covered not only trade in goods, but also trade in services.

Moreover, it had the aim of introducing some reforms to the GATT system to adapt it for the contracting parties' needs: for example, there were the purposes of developing the GATT 1947 decision-making process and improving the existing system's

---

[210] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).

[211] GATT 1947, Article XXV, entitled "Joint Action by the Contracting Parties".

[212] Jhon H. Jackson, *The World Trade Organization: Constitution and Jurisprudence* (London: Royal Institute of International Affairs, 1998)*, 24.*

relationships with the International Monetary Fund and the World Bank in order to reach a better understanding in the worldwide global economy's policymaking[213].

At a first stage, Contracting Parties agreed that they would meet once every two years for implementing GATT 1947.

Two years later, instead, Renato Ruggiero, the Italian Prime Minister in 1990, suggested the creation of a new international organization for trade. Some months later, in April 1990, the idea of the establishment of a "World Trade Organization" was formally proposed by Canada; the European Commission proposed a draft too, aiming at the creation of a "Multilateral Trade Organization".

The common idea was to provide a strong and institutional framework for the implementation, into the GATT 1947, of the results of the Uruguay Round.[214]

However, the United States and some developing countries did not support these proposals, since they were afraid of losing power and they did not want to "have their hands tied".[215]

The Uruguay Round took longer than expected, and finally, more than a year later, the European Community, Canada, and Mexico proposed a joint draft for the establishment of an international trade organization. This was the basis for what resulted, in December 1991, in the draft Agreement Establishing the Multilateral Trade Organization. The agreement was part of the Dunkel Draft, which was the Draft Final Act (named after the Director-General of the GATT at that time).[216]

Still, the United States never supported the establishment of a multilateral trade organization during the Round. It was only with the Clinton administration in 1993 that they agreed to its participation.

---

[213] GATT MIN.DEC, *Ministerial Declaration on the Uruguay Round,* dated 20 September 1986, Part I, Section E, "Functioning of the GATT System".

[214] GATT Doc. No. MTN.GNG/NG14/W/42, *Communication from the European Community,* dated 9 July 1990, 2.

[215] John H. Jackson, "Strengthening the International Legal Framework of the GATT-MTN System: Reform Proposals for the New GATT Round." *The New GATT Round of Multilateral Trade Negotiations: Legal and Economic Problems,* edited by E.-U. Petersmann and M. Hilf, 3-23. Studies in Transnational Economic Law, vol. 5. (Deventer, the Netherlands: Kluwer Law and Taxation Publishers, 1988).

[216] GATT Doc. MTN.TNC/W/FA, *Draft Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations*, 20 December 1991.

In April 1994, the WTO Agreement was signed in Marrakesh. It entered into force on January 1st, 1995 and it was conceived as the "greatest achievement in institutionalized global economic cooperation".[217]

In establishing the World Trade Organization, the contracting parties agreed to pursue the growth in living standards, the assurance of full employment, the growth of real income and effective demand, the development of production, and the improvement of trade in goods and services.

Moreover, all the actions of the WTO have to take into consideration both the principle of sustainability and the needs of the economies of developing countries, in order to save necessary resources and to preserve and protect the environment. This aspect stressed by the Preamble is considered one of the most important innovations in respect of the GATT 1947.[218]

In this term, the Panel in *China – Rare Earths (2014)* stated that interpretations of the WTO agreements which "resulted in sovereign States being legally prevented from taking measures that are necessary to protect the environment or human, animal or plant life or health would likely be inconsistent with the object and purpose of the agreement".[219]

2.1 WTO structure

The WTO is composed by 164 member States, representing almost all the actors of the international trade.

However, the process for accession to the WTO is complex. It starts with the negotiation of a "ticket of admission", in which the Government applying for membership should describe all aspects of its trade and economic policies and referred it to the working party dealing with the country's application. Also parallel bilateral market access

[217] Gary P. Sampson (ed), "Overview", *The Role of the World Trade Organization in Global Governance*, (Tokyo: United Nations University Press, 2001): 5

[218] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).

[219] Panel Report, *China – Rare Earths (2014),* para. 7.114.

negotiation with WTO members take place and a draft membership treaty "protocol of accession" is adopted.

The documents deriving from these negotiations are presented to the WTO General Council or the Ministerial Conference and if a two-third majority of WTO members vote in favour, the applicant can sign the said protocol and accede to the Organization.

In many cases, the agreement should be ratified by the national parliament before membership is considered complete[220].

The highest-level decision-making body is the Ministerial Conference, which meets at least once every two years.

Below this organ there is the General Council, which exercises the functions of the Ministerial Conference in between its sessions and meets several times a year. It also meets as the Dispute Settlement Body (DSB) and the Trade Policy Review Body (TPRB).

Then, specialized councils and manifold committees, working parties and working groups operate at lower levels.[221]

The WTO Director-General heads the WTO Secretariat, based in Geneva with around 630 staff members, and its main duties are to supply technical support for the various committees and the ministerial conferences, and to provide technical assistance for developing economies, in addition to analyze world trade and to explain WTO activities to the public and media.

Regarding the decision-making process, the WTO is a so-called "Member-driven" organization, meaning that the agenda, the proposals, and the decisions are made by all members.

The Director-General or the WTO Secretariat can, on the other hand, make the functions of "honest broker" in the political decision-making process, or they can act to facilitate it.

Through their activities they can be the main contributors for reaching consensus among the members, in case of important decisions or specific agreements.

---

[220] WTO, "How to join the WTO: the accession process", https://www.wto.org/english/thewto_e/whatis_e/tif_e/org3_e.htm#join

[221] *Ibid.*

The WTO decision-making process has been criticized over the years for not being democratic nor transparent or adequately accountable. The main reason of the complaints lies in the fact that there is not a permanent body with the function to guarantee a dialogue between the Organization and the civil society. Moreover, there is no core body which can ensure a slight and rapid process of decision-making or negotiations, but all 164 Member States representatives.

For this reason, when there is the need to make a decision on a controversial issue, it is practically impossible to involve all the Members at the same time. On these occasions the "green room meeting" mechanism is used,[222] chaired by the Director-General, through which the heads of delegations seek consensus informally.[223]

In the Green Room, ministers, ambassadors or senior officials, including the coordinators of the major groups in the WTO meet each other, ensuring a whole representation of all positions, countries, and regions within the negotiations. The informal way of conducting the negotiations has the aim to provide different approaches to solving the most challenging issues. Indeed, sensitive political issues are dealt with during the Ministerial Green Room consultations, such as tariff cuts, or the degree of flexibility of subsidy cuts, etc.

After the consultations, the coordinators make reports for their groups about the results of the meetings. Group members can approve or disapprove the outcomes and they can also ask the coordinators to return to the Green Room for clarifications, revisiting the proposals, entering new requests, or for negotiations to be put into different terms. In particular, if small groups of countries have specific concerns, the Director-General, or facilitators, can consult with the groups in order to reach a compromise.[224]

Moreover, when talking about the WTO decision-making process, a distinction has to be made between decision-making in theory and in practice. A standard decision-making procedure is provided by the Agreement establishing the WTO as a default procedure. Otherwise, some special procedures for specific decisions are provided. Under

---

[222] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).

[223] *Ibid.*

[224] World Trade Organization, *Doha Development Agenda: July 2008 Package: How the meeting was organized.* https://www.wto.org/english/tratop_e/dda_e/meet08_org_e.htm (accessed August 1, 2020).

these procedures, the Member States should take decisions by consensus, or, if it cannot be reached, by expressing their vote.[225]

According to the voting system, every member has one vote and the European Union has a number of votes equal to the number of the EU Member States (currently twenty-seven). But in practice, the decisions are reached essentially by consensus. This is because it is considered the most fundamental, democratic, systematic guarantee of equality.

However, sometimes this decision-making method causes difficulties or even renders the entire process useless, since sometimes a consensus may be unreachable due to the undeniable challenge of finding a solution which satisfies everyone.[226]

2.2 WTO sources of law

International trade and, more generally, economic globalizations are the keys for the development of the economy of all the countries. In order to improve international trade and the growing of economy, some steps have to be fulfilled: it is essential a good national governance; the reduction of trade barriers; international cooperation on the side of global governance in international trade and economy; and also aid for development.[227]

In order to bring prosperity to all the developed and developing economies, international rules on trade are of vital importance.

Indeed, an international legislative framework is needed in order to avoid a country from issuing trade-restrictive measures, for ensuring the stability, security, and predictability of the various trade policies to investors and traders, for protecting societies' values and interests and for promoting equity, equality, and fairness in international economic relations.

To attain these objectives, WTO provides five groups of rules. They are as follows: non-discrimination on market access regarding unfair trade, rules governing the relationship between trade liberalization and other general interests, and institutional and

[225] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).
[226] *Ibid.*
[227] *Ibid.*

procedural laws. Consequently, WTO law has become a complex and broad body of norms. [228]

The main source of WTO law is the *Marrakesh Agreement Establishing the World Trade Organization,* which has been recognized as the most wide-ranging and ambitious international trade agreement ever concluded.

It is made of a short basic agreement of sixteen articles and other agreements which are included into the annexes of the Agreement: among these annexes there are the General Agreement on Tariffs and Trade 1994 (GATT 1994), the General Agreement on Trade in Services (GATS), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS *Agreement*), and the Understanding on Rules and Procedures for the Settlement of Disputes (DSU).[229]

The GATT 1994 is the agreement containing provisions regarding international trade in goods. It consists of provisions, protocols and certifications which provide the rules for much of world trade of goods. In particular: protocols and certifications relating to tariff concessions; protocols of accession; decisions of the contracting parties; various Understandings (such as the Understanding on the Interpretation of Article II:1(b) of the General Agreement on Tariffs and Trade 1994; Understanding on the Interpretation of Article XVII of the General Agreement on Tariffs and Trade 1994 etc.); the Marrakesh Protocol to GATT 1994 and in conclusion, it contains explanatory notes.[230]

Then, there is the GATS which was inspired by the same objectives as its counterpart in merchandise trade, the General Agreement on Tariffs and Trade (GATT): to create an efficient and secure system of international trade rules; to guarantee fair and equitable treatment of all the members, fulfilling the principle of non-discrimination; to encourage the economic activity through guaranteed policy bindings; and to enhance trade and development through progressive liberalization.[231]

---

[228] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).

[229] *Ibid.*

[230] WTO, *General Agreement on Tariffs and Trade 1994,* https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm (accessed January 09, 2021).

[231] WTO, *The General Agreement on Trade in Services (GATS): objectives, coverage and disciplines*, https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm (accessed January 09, 2021).

It contains provisions which apply in principle to all service sectors, with two exceptions. The first one is provided by Article I (3) of the GATS excludes from the scope of the Agreement the "services supplied in the exercise of governmental authority": services that are supplied neither on a commercial basis nor in competition with other suppliers. The second one is laid down in the Annex on Air Transport Services, which excludes from coverage measures affecting air traffic rights and services directly related to the exercise of such rights.[232]

The TRIPS Agreement is defined as the most comprehensive multilateral agreement on intellectual property to date. Its provisions cover different areas of intellectual property: copyright and related rights (i.e. the rights of performers, producers of sound recordings and broadcasting organizations); trademarks and service marks; geographical indications and appellations of origin; industrial designs; patents, and also the protection of new varieties of plants; the layout-designs of integrated circuits; and undisclosed information, including trade secrets and test data.[233]

Finally, the Dispute Settlement Understanding - DSU is the main WTO agreement on settling disputes and it is regarded by the World Trade Organization as the basis of the multilateral trading system, and as the organization's "unique contribution to the stability of the global economy". It is considered as necessary too, because, without a means of settling disputes, the rules-based system would be less effective for the non-enforcement of the provisions. The WTO's procedure emphasizes the rule of law, and it makes the trading system more certain and reliable. The main characteristics of the system are that it is made up of clearly-defined rules, and it is provided of timetables for completing a case. Another feature is that first rulings are made by a panel but are endorsed (or rejected) by the WTO's full membership, and Appeals based on points of law are allowed.[234]

---

[232] *Ibid.*

[233] WTO, *Overview: the TRIPS Agreement*, https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm (accessed January 09, 2021).

[234] WTO, *Understanding the WTO: Settling Disputes: a unique contribution, https://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm* (accessed January 09, 2021).

2.3 WTO functions

In the Preamble to the Agreement establishing the WTO, the objectives pursued by the Organization and the ways they are achieved are stated, namely the reduction of barriers to trade and the abolition of discriminatory behaviors in international trade relations.[235]

Article II:1 of the Agreement establishing the WTO states the primary scope of the Organization, so as "to provide the common institutional framework for the conduct of trade relations among its Members in matters related to the agreements and associated legal instruments included in the Annexes to [the] Agreement".[236]

Article III, instead, delineates the functions of the WTO.

First of all, WTO plays a crucial role in implementing the agreement and the related annexes, and it has to facilitate their administration and operation.

Then, the WTO shall provide "a forum for negotiations among its members concerning their multilateral trade relations in matters dealt with under the agreements" that form part of the Uruguay Round WTO Agreement.

It also provides the establishment of a forum for additional negotiations among the members, dealing with multilateral trade relations by including a framework to implement the outcomes of those negotiations.

A crucial function of the WTO is the one related to the administration of the Understanding on Rules and Procedures Governing the Settlement of Disputes (Dispute Settlement Understanding or "DSU"), included in the Annex II of the Agreement establishing the WTO, which is the object of a specific insight in the following paragraph.

Another function appointed to the World Trade Organization is the administration of the Trade Policy Review Mechanism (TPRM)[237], which has the purpose of contributing to the improvement of adherence to rules and trade policy practices by the Member States, simplifying the functioning of the multilateral trading system[238].

---

[235] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).

[236] WTO Agreement, Article II:1.

[237] WTO Agreement "Trade Policy Review Mechanism", Annex 3.

[238] WTO Agreement "Trade Policy Review Mechanism", para. A(i).

It promotes better transparency in members' trade policies and practices through the achievement of a greater awareness in the understanding of said policies.[239] In developing countries' framework, trade policy reviews aim at identifying and assisting with the technical expertise of the other countries.

Follow-up workshops may be provided in order to incentivize countries to discuss the results of the reviews and to conform their trading regimes in accordance with the international standards promoted by the WTO.[240]

According to Article III:5 of the Agreement establishing the WTO, another function of the WTO is to collaborate with the International Monetary Fund (IMF), the International Bank for Reconstruction and Development, and its related agencies in order to ensure global economic policy-making coherence.[241]

To comply with this function, the WTO has signed various agreements with the IMF and the World Bank, providing for consultations between the WTO Secretariat, the IMF, and World Bank offices to guarantee the exchange of information between the organs, working together on a day-to-day basis to provide technical assistance to developing countries.

Furthermore, they are part of the Enhanced Integrated Framework for Trade-Related Technical Assistance (EIF) along with UNCTAD (*United Nations Conference on Trade and Development)*, the ITC (*International Trade Center)*, and the UNDP (*United Nations Development Programme)*, with the goal of enhancing the expansion of the exports of least-developed countries.[242]

Moreover, the WTO, in compliance with the Article V:1 of the Agreement establishing the WTO, has to collaborate with other international organizations: indeed, it is established that "The General Council shall make appropriate arrangements for effective cooperation with other intergovernmental organizations that have responsibilities related to those of the WTO."[243]

Besides, it has to cooperate with non-governmental organizations (NGOs) as well, since it is stated that "The General Council may make appropriate arrangements for

[239] *Ibid.* pp. 7-11.
[240] WTO Annual Report 2016, 88.
[241] Marrakesh Agreement Establishing the World Trade Organization, Article III:3.
[242] WTO Annual Report 2016, 112.
[243] Marrakesh Agreement Establishing the World Trade Organization, Article V:1.

consultation and cooperation with non-governmental organizations concerned with matters related to those of the WTO".[244]

One implicit function of the WTO, not mentioned in Article III of the Agreement establishing the WTO is to provide technical assistance to developing countries, in order to make their integration into the world trading system possible.[245]

2.4 WTO Dispute Settlement System

The WTO Dispute Settlement System is recognized as one of the most fruitful outcomes of the Uruguay Round, having made a remarkable step forward to the framework of the "progressive judicialization" of the international trade disputes' settlement.[246]

According to Article 3.2 of the DSU: "The dispute settlement system of the WTO is a central element in providing security and predictability to the multilateral trading system."[247] An efficient settlement of dispute in the WTO's framework is necessary for the functioning of the overall system as well as for maintaining the balance between contracting members' rights and duties.

The DSU was conceived both to safeguard the rights and the obligations of members stated in the agreements and to provide interpretations for the application of those agreements.[248] In line with the purpose of guaranteeing balance, it is invested with the power to add, reduce, or modify the same rights and obligations provided within the agreements.[249]

Regarding the various aspects of the WTO Dispute Settlement System, it should be highlight that the jurisdiction is compulsory, exclusive and contentious in nature. Its scope is so wide to govern all the disputes arising under, not only the Agreement establishing the WTO and the Dispute Settlement Understanding (DSU), but also under

---

[244] Marrakesh Agreement Establishing the World Trade Organization, Article V:2.

[245] World Trade Organization, Ministerial Conference, *Doha Ministerial Declaration,* 9-14 November 2001, WT/MIN(01)/DEC/1, Doha, 20 November 2001, para. 38.

[246] Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017).

[247] Dispute Settlement Understanding, Article 3.2.

[248] Dispute Settlement Understanding, Article 3.3.

[249] Dispute Settlement Understanding, Article 3.2.

the multilateral Agreements and the plurilateral agreement on trade in goods, adopted under the TRIPS Agreement and the GATS.[250]

Only WTO Members can have access to the WTO dispute settlement system, while NGOs, legal persons, associations or individuals have no direct access to it. The access is granted whenever the benefits derived from the Agreements are impaired, nullified or denied to the claimant. Furthermore, the complainant usually claims a violation of the WTO law by the respondent, filing a violation complaint. When the violation is shown, the nullification or impairment of the benefit is presumed; otherwise, the complainant may file a complaint addressing the non-violation.[251]

The main object and purpose of this system is the rapid settlement of disputes between its Members, granting security, predictability and reliability to the trading system.[252]

The features of the WTO Dispute Settlement System, apart from the compulsory and the exclusive jurisdiction, are the singular, extensive and incorporated nature of the system. Another characteristic of the system is the provision of multiple methods to solve disputes arisen from Members: consultations, negotiations, adjudications by panels and the Appellate Body, arbitration, good office, conciliation and mediation. Furthermore, the system of consultations, which have "mutually acceptable solutions" as outcomes, are preferred to adjudications.[253]

In case of breach of WTO laws, the Dispute Settlement Understanding (DSU) provides three remedies: first of all, the withdrawal or the modification of the measure inconsistent with the WTO provisions; then, two temporary remedies are provided, and in particular the compensation and the retaliation (the suspension of concessions, benefits or other obligations)[254].

WTO Dispute Settlement System comprises political and judicial institution.

The Dispute Settlement Body belongs to the first category, since it is in charge of establishing panels, of adopting panel and Appellate Body reports and of authorizing the measure of retaliation in case of non-compliance to WTO laws.

---

[250] *Ibid.*
[251] *Ibid.*
[252] *Ibid.*
[253] *Ibid.*
[254] *Ibid*

The dispute settlement panel and the Appellate Body, instead, are two judicial-type institutions, before which the actual adjudication of disputes is brought.

At the first-instance level the competence is up to the Dispute Settlement Body, while, at the appellate level the Appellate Body is competent.[255]

Panels are bodies settled for adjudicating a specific dispute, under the specific request of the complainants (or by reverse consensus, after the second meeting in which the request for the establishment of a panel is discussed), and they are disbanded once the dispute is solved: they are the so-called *ad hoc* panels.

Usually, the composition of the panels is decided by the parties by mutual agreement, but if the latter cannot be reached, each party, until twenty days from the establishment of the panel, may make a request to the WTO Director-General to appoint the members of the panel.

Those members are well-qualified governmental and/or non-governmental individuals and they must not have the same nationality of the parties neither of third parties to the dispute. The main reason of this choice is that they have to be impartial and independent in their decisions. Furthermore, WTO DSU tries to avoid conflict of interests and it pursues the principle of confidentiality of proceedings.[256]

The Appellate Body, instead, can be defined as a permanent international body, made of seven individuals of recognized authority appointed by the Dispute Settlement Body and in charge for a mandate of four years which is renewable once.

According to the WTO Dispute Settlement Rules of Conduct, their mandate must respect the principle of independence and impartiality, conflicts of interests have to be avoided and the confidentiality of proceedings have to be respected.

The Appellate Body in its decisions has the power to uphold or modify the results of the panels at first instance, and in some occasions, it also extended the legal analysis in fields not touched by the panels. Thus, the main steps of the WTO dispute settlement process are the consultations, the panels proceedings, the Appellate Body Proceedings, the implementation and the enforcement. [257]

---

[255] *Ibid.*
[256] *Ibid.*
[257] *Ibid.* at 300.

In conclusion, it should be noted that the WTO has one of the most active international dispute settlement mechanisms in the world: since 1995, 598 disputes have been brought to the WTO and over 350 rulings have been issued[258].

3. Restrictions on Data Flows in International Trade: an introduction

During the last few years, we have experienced an enormous growth of the digital services industry.

Internet has become a global stage in which technology companies and new figures of entrepreneurs take act on their interests.[259] Digital services now include the most diverse fields on the internet; from cloud computing to movie streaming or legal services, etc.[260]

The nature of world trade has undoubtedly changed, as nowadays it is mainly characterized by globalization and the decentralization of the production process. This new way of carrying out business is facilitated and endorsed by data flow.[261]

Technology is growing exponentially, giving the possibility to transfer huge volumes of data. As a result, new concerns regarding cybersecurity, invasion of privacy, and the commercialization of people's data, arise. In an attempt to anticipate these new regulatory challenges, as anticipated above, every state has adopted a proper approach in its domestic legislation.[262]

---

[258] WTO, "Dispute Settlement", https://www.wto.org/english/tratop_e/dispu_e/dispu_e.htm

[259]Congressional Research Service, *Digital Trade and US Trade Policy*, 21 May 2019, https://fas.org/sgp/crs/misc/R44565.pdf (accessed August 1, 2020); eBay Inc and Sidley Austin LLP, *Commerce 3.0 for Development: The Promise of the Global Empowerment Network,* October 2013, https://www.ebaymainstreet.com/sites/default/files/eBay_Commerce-3-for-Development.pdf (accessed August 1, 2020)

[260] Jessica Nicholson and Ryan Noonan, "Digital Economy and Cross-Border Trade: The Value of Digitally- Deliverable Services", *US Department of Commerce Economics and Statistics Administration*, ESA Issue Brief no 1-14, (2014): 1.

[261] ICC Commission on Trade and Investment Policy and ICC Commission on the Digital Economy, "Trade in the Digital Economy—A Primer on Global Data Flows for Policymakers" *lnternational Chamber of Commerce (ICC)*, 2016, Policy Paper 103/330, 373/560 1 <https://iccwbo.org/publication/trade-in-the-digital-economy/> (accessed August 3, 2020); Joshua P. Meltzer, "A New Digital Trade Agenda". *E15Initiative*. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2015. www.e15initiative.org/. (accessed August 3, 2020)

[262] Nivedita Sen, "Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?" *Journal of International Economic Law,* Oxford University Press, Vol. 21 No. 2, (2018): 323, 324.

With the increase in the number of digital services offered, governing restrictions on cross-border trades in those services have increased too.[263] Most of them are non-tariff measures[264], such as specific laws and regulations, technical standard requirements, and qualification requirements.[265]

One of the most commonly used restriction measures in digital international trade is the one referred to personal data protection.

In general, the restrictions on data flows, also known as "data restrictive measures", are a series of governmental decisions, regulations, national rules, and administrative policies which limit the flow of personal data through the internet and consequently, across territorial borders[266] , and which can be direct or indirect in nature.

For instance, some direct restrictive measures can be those that block digital services or digital contents[267]. These take the form of laws which require the storage of data on domestic servers.[268]

Indirect restrictions, instead, can be, for example, the need to comply with specific conditions under domestic data protection legislation and cybersecurity law.[269]

In general, the following four categories of restrictive measures can be identified:

"Ban on the transfer of data abroad (data can never leave the country);

- Local processing requirement (data can leave the country but the main processing has to be done locally);

- Local storage requirement (a copy of the data has to be stored locally); and

---

[263] Martina Ferracane, Hosuk Lee Makiyama and Erik van der Marel "Digital Trade Restrictiveness Index", *European Centre For International Political Economy, Digital Trade Estimates.* <http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2018/09/DTRI-final.pdf> 5. (accessed August 3, 2020)

[264] Philippa Dee, "A Compendium of Barriers to Services Trade" (World Bank, 2005): 3-4.

[265] World Trade Organization, *World Trade Report 2012* (2012): 123-6.

[266] Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", *OECD Digital Economy Papers,* No. 187, OECD Publishing, (2011): 12.

[267] Internet Code of Practice (Singapore), 1 November 1997, art 4; US Department of Homeland Security, "DHS Statement on the Issuance of Binding Operational Directive 17- 01" *Homeland Security,* Press Release, September 13, 2017, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational- directive-17-01 (accessed August 4, 2020).

[268] Beschluss des Rates der IT-Beauftragten der Ressorts (Germany), Beschluss Nr 2015/5, July 29, 2015; Decree on the Management, Provision and Use of Internet Services and Online Information (Vietnam), Decree No 72/2013/ND-CP, art 4.4, art 5, July 15, 2013; Undang-Undang Tentang Pelayanan Publik (Indonesia), Law No 25/2009, July 18, 2009.

[269] Cybersecurity Law (People's Republic of China), National People's Congress, June 1, 2017; Law on Network Information Security (Vietnam), Law no 86/2015/QH13, art 16 – art 20, July 1, 2016.

- Conditional flow regime (data can travel abroad only under certain conditions, such as consent of the data subject)"[270].

From these premises two policy questions arise. First of all, if restrictive measures are already covered by the current trade regime, and if so, whether the measures may violate rules in force or if they are considered as exceptions to the existing ones.
The second question is about the necessity and the opportunity of multilateral rulemaking, keeping the aim of protection of data flows in mind. The way the normative framework may be structured and developed comes up, constituting, at the same time, a legitimate exception to public policy.[271]

As anticipated, WTO system is in charge to regulate almost the totality of worldwide trade in goods and services. It also provides, as mentioned above, a dispute resolution mechanism with the function to enforce members' respect to their commitments. The procedure requires that when a country takes a measure which is considered in violation to WTO commitments and obligations, they can rely on the dispute settlement mechanism.[272]

However, until today, there is an absence of disputes at the WTO dealing with data-related trade.

The possible reasons could be that trade in relation with data flows is a recent phenomenon and members try to avoid disputes on data restrictive measure since they recognize the necessity to regulate the internet.[273]

---

[270] Martina Ferracane, "Data Flows & National Security: A conceptual framework to assess restrictions on data flows under GATS security exception", *GigaNet: Global Internet Governance Academic Network, Annual Symposium,* 2018.

[271] Nivedita Sen, "Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?" Journal of International Economic Law, Oxford University Press, vol. 21(2) (2018): 323, 324.

[272] Martina Ferracane, "Data Flows & National Security: A conceptual framework to assess restrictions on data flows under GATS security exception", *GigaNet: Global Internet Governance Academic Network, Annual Symposium,* 2018. The Author suggests that There have been two trade disputes that indirectly address data flows: United States-Measures Affecting the Cross-Border supply of Gambling and Betting Services and China-Measures Affecting Trading Rights and Distributions Services for Certain Publications and Audiovisual Entertainment Products, that will be further analyzed.

[273] Communication from the US, *Joint Statement on Electronic Commerce*, WTO Doc INF/ECOM/23 April 26, 2019; Communication from Japan, *Joint Statement on Electronic Commerce Initiative*, WTO Doc INF/ECOM/4 March 25, 2019.

Some governments also have complained about potential national treatment implications. The DG Trade Commissioner, Malmström, stated that "restrictions on cross-border data flows inhibit trade of all kinds: digital and non-digital, products and services. We cannot just pretend that this does not exist, or that data has nothing to do with global trade".[274] Furthermore, there are some concerns about the fact that cross-border data flows can qualify as a trade restriction because they have been explicitly addressed as such in a few trade agreements.[275]

The following paragraphs are focused on the concrete application of GATS provisions in the framework of digital international trade.

3.1 The application of GATS to Digital International Trade

Despite attempts to include references on data flows under the Work Program on Electronic Commerce by WTO in 1998, as of today there are no rules on data flows being negotiated in the WTO.

In order to further investigate the topic, a preliminary issue to examine is which areas are covered by the General Agreement on Trade in Services and, consequently, whether GATS applies to data-restrictive measures.

The General Agreement on Trade in Services, after being signed by all WTO Members, was definitively adopted in 1994 and incorporated into the Final Act of the Uruguay Round.

The development of new technologies and the enhancement of the internet have been the engine through which the services have been tradable and performable not only at local level, but also at international level, such as the bank activity or the elaboration of data.[276]

In the GATS, three main elements can be recognized: the framework agreement containing the general rules and obligations applicable to all Members; the national

[274] Cecilia Malmström, *Speech on TTIP and Trade,* Berlin 2016.
[275] Communication from the US, *Joint Statement on Electronic Commerce*, WTO Doc INF/ECOM/23 April 26, 2019; Communication from Japan, *Joint Statement on Electronic Commerce Initiative*, WTO Doc INF/ECOM/4 March 25, 2019.
[276] Treccani, "GATS (General Agreement on Trade in Services)", *Dizionario di Economia e Finanza (2012),* available at https://www.treccani.it/enciclopedia/gats_%28Dizionario-di-Economia-e-Finanza%29/ (accessed September 27th, 2020).

schedules, which contain countries' commitments on access of foreign suppliers to their domestic markets; the Annexes, dedicated to specific sectors, such as telecommunications, finance, public services, etc.[277]

Among the main principles, accepted by all the Parties to the Agreement, there is the transparency of the rules and the regulations which govern the access to the markets and the most-favored-nation clause, which aims to ensure that there are not any preferential treatments among WTO countries.[278]

For the purpose of this research, since restrictions on data flow have a direct impact on trade in services, it can be said that GATS is the agreement that best fits the topic analyzed.[279]

According to the words of the agreement, GATS applies to "measures by Members affecting trade in services".[280] Trade in service is referred to as the supply of a service. The latter is defined in broad terms including the "production, distribution, marketing, sale and delivery of a service".[281]

Governments are free to regulate the internet and to pursue policy objectives under the GATS, even if they lead to restrictions of trade.

Anyway, in order to be legitimate, the restrictive measures have to be not only necessary, but also efficient and effective, and they have to reach a high grade of reasonableness.[282]

This research aims also at investigating the role of the GATS as an equalizer between free trades and the pursuit of members' policy objectives. Indeed, it has to guarantee that restrictive measures that are taken are essential to the pursuit of policy objectives and that the system is not taken advantage of for the benefit of domestic suppliers.

---

[277] *Ibid.*

[278] *Ibid.*

[279] Martina Ferracane, "Data Flows & National Security: A conceptual framework to assess restrictions on data flows under GATS security exception", *GigaNet: Global Internet Governance Academic Network, Annual Symposium,* 2018.

[280] General Agreement on Trade in Services, art I:1.

[281] General Agreement on Trade in Services, art XXVIII(b).

[282] William J. Drake, Vinton G. Cerf, Wolfgang Kleinwächter, "Internet Fragmentation: An Overview" *Future of the Internet Initiative White Paper*, World Economic Forum, (2016): 44-5.

In particular, it can be argued that the GATS has an impact on digital trade for different reasons. The main argument on the application of this agreement relies on the fact that communication services, providing the access to digital trade, fall under the scope of the GATS.[283]

Then, GATS governs several sectors of delivery and it has been declared technologically neutral.[284]

The third reason could be that the execution of electronic transactions needs infrastructure services, such as payments. These too fall under the scope of the GATS.[285]

Any Member agrees to the liberalization of service sectors, such as education, auditing, or legal services, etc. The commitments are then listed in specific schedules of service commitments. Thus, what is covered or not by a WTO member schedule of service is up to the single country.[286] Each service can be provided either physically or electronically and if unlimited market access commitments are undertaken, then, all the means of delivery shall be allowed.[287]

According to Article VI of the GATS "in sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner." Furthermore, the provision authorizes the Council for Trade in Service to establish and develop proper disciplines to ensure that the measures, taken by the States, requiring determined provisions or proper technical standards, don't reveal themselves as unnecessary barriers to trade.[288]

Furthermore, WTO Members have submitted the "Reference Paper", which contains some rules for preventing anti-competitive behaviors in the sector of telecommunications. The reference paper provides an independent regulatory agency for supervising the respect of the basic recognized principles in the WTO (non-

[283] Taunya L. McLarty "Liberalized Telecommunications Trade in the WTO: Implications for Universal Service Policy", *Federal Communications Law Journal*, Vol. 51 (1998): 1-7.
[284] WTO Panel Report, *US – Gambling*, WT/DS285/R, para. 6.285.
[285] Bashar Malkawi, "Digitalization of Trade in Free Trade Agreements with Reference to the WTO and the USMCA: A Closer Look." *China and WTO Review*, (2019).
[286] Ruosi Zhang, "Covered or Not Covered: That Is the Question - Services Classification and Its Implications for Specific Commitments under the GATS", *WTO Staff Working Papers from World Trade Organization (WTO), Economic Research and Statistics Division,* No. ERSD-2015-11, f (2015).
[287] WTO Appellate Body Report, *US – Gambling*, WT/DS285/AB/R, 239.
[288] General Agreement on Trade in Services, art VI.

discriminatory principle, transparent access, etc) and the fair running of telecommunication markets.[289]

Of great importance in the field of digital trade, there is also the Information Technology Agreement (ITA), which aims at establishing a common policy regarding trade in information technology (IT) goods.

Through this agreement WTO Members agreed to reduce their tariffs on IT-goods for the achievement of a tariff-free policy since 2000.[290] This obligation refers to a list of 180 products of information technology, divided into the following five categories: computers, software, semiconductors, printed circuit boards and telecommunication equipment.

Furthermore, during the Ministerial Conference in 1998, WTO Members, influenced by US, decided to agree on a digital trade work program.[291]

Under the WTO work program on electronic commerce, the notion of digital trade comprises the production, marketing, selling, delivering and distribution of goods and services through electronic means.

The digital trade transactions are divided in the marketing (advertising and searching phase); in the transactions (ordering and payment phase), and in the delivery phase.

However, WTO Work Program on Electronic Commerce has not taken many steps forward mainly due to the question of categorization of products. The issue relies on products which, before the digitalization of commerce and the development of new technologies, were sold as "physical", but that now can be sold also as "digital" products.

WTO Members' approaches differ on whether these products shall fall into the General Agreement on Tariffs and Trade (GATT) or shall be treated as services, falling into the GATS' scope.[292]

---

[289] Charles Owen Verrill, Jr., Peter S. Jordan, Timothy C. Brightbill, "International Trade", *International Lawyer* Vol. 32 (1998): 319-324.

[290] *Ibid.*

[291] WTO Secretariat, *Development Implications of Electronic Commerce*, WT/COMTD/w/51, November 23, 1998.

[292] Kristi L. Bergemann, "A Digital Free Trade Zone and Necessarily-Regulated Self-Governance for Electronic Commerce: The World Trade Organization, International Law, and Classical Liberalism in Cyberspace", *Marshall Journal of Computer and Information Law* Vol. 20, (2002): 595-601.

For instance, a newspaper can be bought online and delivered physically. It is therefore, considered a good for WTO trade rules scope of application. In this case it is subject to the GATT. If the newspaper, instead, is delivered electronically, it is not clearly determined whether it follows the goods or services policy. In the first case, it would be subject to trade restrictions under GATT, such as tariffs restrictive measures.[293] Otherwise, it should be subject to GATS restrictions, regarding market access barriers and discriminatory domestic regulations. On this point, according to the United States' position, online delivered products have to be considered goods. The European Union, on the contrary, holds the opinion that they should be considered services.[294]

There have been several meetings to solve this debate, but the issue is still object of intense study.[295]

3.1.1 WTO Digital International Trade Case Law under GATS provisions

As already highlighted above, currently, there have been no disputes at the WTO specifically related to restrictions on data flows, but there have been two disputes that indirectly address the topic, which are quite emblematic also in order to demonstrate the possibility to apply GATS provision to digital trade and to data restrictive measures.

The WTO cases in questions are United States-Measures Affecting the Cross-Border supply of Gambling and Betting Services (hereafter US-Gambling), and China-Measures Affecting Trading Rights and Distributions Services for Certain Publications and Audiovisual Entertainment Products (hereafter China-Publications and Audiovisual Products).

The first case mentioned dealt with the U.S. restrictions on cross-border internet gambling services. In that occasion, Antigua and Barbuda claimed that U.S. internet gambling restrictions and restrictions against credit card companies on payments to offshore gambling outlets were in violation of the GATS commitments agreed on by the U.S.

---

[293] Stewart A. Baker, Peter Lichtenbaum, Maury D. Shenk, Matthew S. Yeo, "E-Products and the WTO*"* *International Lawyer* Vol. 35, (2001): 5-7.

[294] *Ibid.*

[295] Daniel Pruzin, "U.S. Holds E-commerce Talks with WTO Partners, Covering Nature of Digital Products", *International Trade Daily,* Bureau of National Affairs, June 13, 2001.

According to Antigua, US restrictions caused the loss of almost $90 million in a four-year period, from 2000 to 2004. The U.S., indeed, was its principal market and the result of the loss was the failure of 89 internet gambling enterprises in Antigua.[296]

The WTO panel established for that case stated that online gambling restrictions, imposed by the US at the federal and state level, violated its market commitments under its GATS schedule, and in particular under sub-sector 10.D, called "other recreational services".[297]

In particular, the panel confirmed that U.S. commitments mentioned above, covering "other recreational services" did involve gambling services. Consequently, the panel rejected the U.S. defense according to which it never meant to allow the cross-border supply of those services.

The panel argued that the U.S commitment to permit unrestricted market access on recreational services covered every means of delivering, including the Internet. The WTO panel agreed with the defendant on the fact that the U.S. ban, put on cross-border gambling services, may find its justification under the WTO "public morals" protection clause.[298]

Another early case about digital trade was "China – Publications and Audiovisual Products". In this case the WTO Panel ruled on China's commitment in the GATS schedule on "sound recording distribution services", stating that the scope of the Commitment extended to digital sound recordings distributed through non-physical means, such as the internet.[299]

In its argument the WTO panel referred to the principle of progressive liberalization, according to which, WTO members agree on commitments through multiple rounds of successive negotiations, having the scope of liberalizing, always more their services markets.[300] Thus, this implies that distribution covers all the products, tangible and not.

---

[296] Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/AB/R, April 7, 2005.
[297] *Ibid.*
[298] *Ibid.*
[299] WTO Panel Report, *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, August 12, 2009: para. 7.1209.
[300] WTO Appellate Body Report, *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, December 21, 2009: paras. 392-394.

With those two findings, the WTO's ruling started to gain important ground upon the relationship between the WTO and digital trade, demonstrating also that the GATS can cover the WTO disputes on digital trade.

3.2 GATS exceptions on free cross border data flows: an introduction

Measures restricting cross-border data flows could then be assessed as a restriction on cross-border supply of services under GATS provisions, referring to both "traditional" services and digital ones.

In general, privacy protection is one of the most used rationales to restrict cross-border data flows at national level[301].

As mentioned in the first chapter of this thesis, Governments have progressively implemented their legislation on data protection, in order to gain control over the information of their citizens, the way that information is used, transferred and stored.[302]

The majority of those national legislations consist of provisions that restrict the personal data free flow across borders in order to guarantee that digital service suppliers would comply with national data protection standards.[303]

Data protective measures, through the narrowing of personal data flows, can negatively impact on internet openness. In fact, domestic regulations upon privacy and data protection, issuing restrictive measures, have an effect on the open, end-to-end internet structure. To achieve trust in the digital environment is necessary the guarantee of internet privacy and the latter is one of the essential basis for fostering internet openness.[304]

---

[301] ECIPE, "Digital Trade Estimates Database" <https://ecipe.org/dte/database/?country=&chapter=829&subchapter=830> (accessed August 5, 2020).

[302] W. Kuan Hon, *Data Localization Laws and Policy,* (Cheltenham, UK; Northampton, MA, USA: Edward Elgar, 2017): 8.

[303] Shin-yi Peng and Han-wei Liu, "The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?" *Journal of World Trade* Vol.51 No. 2 (2017): 183, 199; W. Kuan Hon, *Data Localization Laws and Policy,* (Cheltenham, UK; Northampton, MA, USA: Edward Elgar, 2017): 2, 48-9; Communication from the African Group, "Work Programme on Electronic Commerce", *Report of Panel Discussion on 'Digital Industrial Policy and Development'*, WTO Doc JOB/GC/133 July 21, 2017.

[304] Dara Hoffman, Elissa How, "Trust in the Balance: Data Protection Laws as Tools for Privacy and Security in the Cloud" 10 *Algorithms* (2017): 47, 55-6; Tatevik Sargsyan, "The Turn To Infrastracture in Privacy Governance" in *The Turn to Infrastructure in Internet Governance,* eds. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, Nanette S. Levinson, (Palgrave Macmillan US, 2015): 189, 198; Anupam Chander and Uyen P Le, "Data Nationalism" *Emory Law Journal* Vol. 64 No. 3 (2015): 677, 730;

Privacy and data protection national measures can have an influence on international trade, since they usually create market access barriers for foreign digital service suppliers, resulting in disadvantages for a fair competitive system.

As known, GATS provides a number of specific grounds for adopting restrictions on data flows based on some objectives: they are enumerated in Article XIV (General Exceptions) and Article XIV bis (Security Exception), as they will be analyzed in the following paragraphs.

Despite the fact that GATS has not been updated to take into specific consideration new technologies issues, and in particular online services and digital services trade, "it is inevitable that the WTO would find itself in the position to adjudicate when certain internet measures would be justified, or not, under the current exceptions"[305].

The following analysis deals with the opportunity to study the national data restrictive measures under the light of these exceptions, in order to find limits to their legitimacy.

3.2.1 General Exceptions under GATS Article XIV

Starting from the General Exceptions under the GATS Article XIV, it can be argued that this Article lists a series of justifications for restrictive measures necessary to be consistent with GATS regime.

First of all, under GATS XIV(a), a measure can be justified for the protection of public morals or for the maintenance of public order: in this case, a restricting flow of data can be necessary according to the Government in order to protect public morals or public order.

Secondly, a measure can be justified under GATS XIV(b), in order to "secure compliance with laws or regulations which are not inconsistent" with GATS and in

---

Jennifer Daskal, "The Un-Territoriality of Data" (2015) 125(2) *Yale Law Journal* Vol.125 No.2 (2015): 326, 329; Christopher Kuner et al, "Internet Balkanization Gathers Pace: Is Privacy the Real Driver?" *International Data Privacy Law* Vol. 5 No. 1 (2015): 1, 2.

[305] Martina Ferracane, "Data Flows & National Security: A conceptual framework to assess restrictions on data flows under GATS security exception", *GigaNet: Global Internet Governance Academic Network, Annual Symposium,* 2018.

particular for "the prevention of deceptive and fraudulent practices", like cyberfraud or cybercrime: in this case, a Government could argue that the retention of certain data within its borders would be necessary to prevent fraud or to prosecute a crime over the internet.

Other grounds for justifying restrictive measures can be the necessity to ensure equitable or effective imposition or collection of direct taxes or for avoiding double taxation.[306]

An exception relevant for this analysis is the one stated at GATS XIV(c) (ii) and, in particular, the reference to the need of "protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts", since in in this case, the Government would argue that certain restrictions on movement of data are necessary to protect the privacy of its citizens.

For example, "if the GDPR were challenged under WTO, the European Union would probably argue that the law is consistent with the GATS obligations and it is justified under the general exception on privacy. The implementation of the law also needs to be proven consistent with the member's obligations"[307].

This topic will be further analyzed in the following chapter of the thesis.

Moreover, under GATS XIV(c)(iii), a measure inconsistent with Members' GATS obligations is provisionally justified if: (a) it is implemented in compliance with "domestic laws and regulations" [308] involving those "relat[ing] to": "(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts" [309]; (b) the "laws and regulation" are consistent with WTO law; (c) the measure result to be necessary to ensure compliance with the above "laws and regulations".[310]

---

[306] General Agreement on Trade in Services, art. XIV.

[307] Martina Ferracane, "Data Flows & National Security: A conceptual framework to assess restrictions on data flows under GATS security exception", *GigaNet: Global Internet Governance Academic Network, Annual Symposium,* 2018.

[308] WTO Appellate Body Report, *Mexico – Taxes on Soft Drinks,* 79.

[309] General Agreement on Trade in Services, art. XIV(c)(iii).

[310] WTO Panel Report, *Colombia – Ports of Entry,* 7.514; WTO Appellate Body Report, *US – Shrimp (Thailand),* 7.174; WTO Appellate Body Report, *Korea – Various Measures on Beef* , 157; WTO Appellate Body Report, *Thailand – Cigarettes (Philippines).*

This provision has been interpreted in various evolutive ways with the purpose to include into its scope different aspects of the right to online privacy. For example, "protection of privacy of individuals" has been interpreted to involve, into the scope of GATS Article XIV(c)(ii), the policy objectives of avoiding different types of online surveillance of individuals carried out by governments without authorization and also the use of personal data by companies and businesses without explicit consent of the user.

Moreover, the term "secures compliance" means that domestic legislations should "enforce obligations contained in [those] laws and regulations".[311]

Indeed, cross-border data processing may be restricted in order to protect data from a third-party illegal use.

However, according to the WTO Appellate Body the wording "securing compliance" does not mean that the result of the measure is guaranteed with "absolute certainty".[312]

Another relevant topic concerns the inclusion of the security exception in various WTO texts. In particular, security exceptions are found in Article XXI of the GATT, Article XIV bis of the GATS, Article 73 of the TRIPS and Article XXIII of the Agreement on Government Procurement (GPA).

GATS Art. XIV bis remains however the most relevant article when dealing with data flows and services.

Looking closely the provision (b)(iii) of GATS security exception, it provides that nothing in the agreement should be interpreted meaning to 'prevent any Member from taking any action which it considers necessary for the protection of its security interests (...) taken in time of war or other emergency in international relations". According to this provision, whoever wants to invoke this exception could justify restrictions on movement of data by affirming that it is "necessary" in order to protect its "essential security interests" because of an "emergency in international relations" that can be the result, for example, of threats of a cyber-attack that could affect the whole country.

It can be said that the WTO jurisprudence has not provided a sufficient degree of clarity when it comes to the interpretation of GATS security exception. This is also

[311] WTO Panel Report, *US — Gambling,* 6.538. WTO Appellate Body Report, *US — Gasoline,* 6.33.
[312] WTO Appellate Body Report, *Mexico – Taxes on Soft Drinks* 72-74; WTO Panel Report, *China —Auto Parts* 7.337.

confirmed by the fact that the WTO judiciary has consistently avoided issuing findings on the merits of this article and consequently it has been mention rarely in trade disputes. For this reason, it is high the level of uncertainty in relation to the interpretation of this clause. The same applies to the security exception provided by Article XXI of the GATT, where few are the cases in which this measure has been referred to.

If a comparison between the measures shall be made, it can be noticed that the security exception differs from the general exceptions on two main grounds: its measures do not explicitly forbid arbitrary or unjustifiable discrimination, and, to claim for the exception, a Member only has to "consider" that its security interests are endangered, so it could appear like a Member can self-interpret its own security interests.[313]

3.2.1.1. Necessity test under GATS Article XIV

The Necessity test of privacy measures under GATS Article XIV consists of: (i) the assessment of the reasonableness and the importance of the values and interests promoted by the measure; and of (ii) an exam regarding "weight and balance" for testing the "importance" of the objectives that the measures are meant to pursue.

In doing so, WTO Panels and Appellate Body have to look at several aspects. For example, they have to examine the effective contribution of the measure to the policy objective, the effects on international trade, and if the complainant have suggested alternatives which would have less restrictive impact on international trade, but at the same time pursue the same policy objectives of the measure at issue. [314]

In the WTO case law, usually, more crucial is the policy objective of a measure, more are the chances for the Panels and the Appellate Body to state the necessity of that measure.[315]

---

[313] Martina Ferracane, "Data Flows & National Security: A conceptual framework to assess restrictions on data flows under GATS security exception", *GigaNet: Global Internet Governance Academic Network, Annual Symposium,* 2018.

[314] WTO Appellate Body Report, *Brazil – Retreaded Tyres* 146, 178; WTO Appellate Body Report, *US – Gambling,* 307; WTO Appellate Body Report, *Korea – Various Measures on Beef*, 164.

[315] WTO Appellate Body Report, *Korea – Various Measures on Beef,* 162.

As noted above, GATS Article XIV(c)(ii) explicitly promotes the protection of privacy, since the pre-internet era, as WTO Members have always been concerned about service suppliers threatening the privacy of their citizens and consumers.[316]

The further step of the legal analysis under GATS Article XIV is the exam of several technical conditions to evaluate whether the measure is necessary to achieve objects related to privacy.[317] An example can be found in the experts' advices about the adequacy of local data storage in the protection of privacy, by which it has been stated that local data storage compromises personal privacy increasing the chances of cyberattacks and illegal surveillance by the governments.[318]

Ultimately, technical information is really important to test the contribution of a measure to privacy-related objectives. WTO Panels' next step consists in the examination of the effects of the restrictive measures in different economic and business operations[319],in the field of international trade.

These measures may impact, in different ways, on several aspects of international trade, making difficult to estimate a direct effect on the business. For this reason, the evidence provided by complainants aim at highlighting the measures' effects on e-commerce, such as surveys' results indicating closer or competitive markets for digital

[316] WTO Appellate Body Report, *US – Gambling,* 304.

[317] WTO Appellate Body Report, *Brazil – Retreaded Tyres,* 210. WTO Appellate Body Reports, *EC – Seal Products,* 5.210.

[318] Tim Maurer, Robert Morgus, Isabel Skierka and Mirko Hohmann, "Technological Sovereignty: Missing the Point?" in *Architectures in Cyberspace* eds. M. Maybaum, A. -M. Osula, L.Lindstöm, (NATO CCD COE Publications, 2015): 53, 61-2; Nigel Cory, "Cross-Border Data Flows: Where are the Barriers and What Do They Cost?" (May 2017): 3 – 4. <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost> (accessed August 5, 2020); Konstantinos Komaitis, "The "Wicked Problem" of Data Localization", *Journal of Cyber Policy* Vol. 3, No. 2 (2017): 355, 361-2; United States International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, Publication number 4716, Investigation Number 332-561, August 2017 (285); Usman Ahmed and Anupam Chander, "Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows" *Think Piece*, E15 Expert Group on the Digital Economy, November 2015 (6-7); W Kuan Hon, Christopher Millard, Jatinder Singh, Ian Walden, Jon Crowcroft, "Policy, Legal and Regulatory Implications of a Europe-only Cloud", *International Journal of Law and Information Technology* Vol. 24, No. 3 (2016): 251, 262.

[319] W Kuan Hon, Christopher Millard, Jatinder Singh, Ian Walden, Jon Crowcroft, "Policy, Legal and Regulatory Implications of a Europe-only Cloud", *International Journal of Law and Information Technology* Vol. 24, No. 3 (2016): 251, 262.

services from abroad, the lack of confidence in foreign digital services or the absence of trust in domestic and local cloud computing facilities.[320]

Through these evidence, the complainants' purpose is to provide Panels of factors which prove the restriction and the obstacles that import-export's services find into the market.[321]

The ultimate step of Panels' investigation is to examine whether the alternatives proposed by the complainant are applicable to the case in question, ensuring the same level of privacy and data protection,[322] and if the less trade-restrictive measures are suitable for the defendant.[323]

For instance, an alternative to data-restrictive measures could be privacy Trustmark and self-certification measures.

The first ones are managed by private parties under the general administration of governmental agencies. An example of privacy Trustmark is the "Truste", an accountability agent recognized in the APEC Cross Border Privacy Rules System (CBPR) as a business organization, established in the US, which is under the oversight of the US government.

Regarding self-certification mechanisms, instead, a relevant example is the EU-Privacy Shield, according to which, US companies can self-declare that their provisions follow EU data protection standards.[324]

These mechanisms are not always real alternatives. In particular, often developing countries do not have proper resources or adequate expertise to develop, manage and maintain self-certification programmes. Furthermore, it happens that governments do not

[320] Economics and Statistics Administration and the National Telecommunications and Information Administration, *Measuring the Value of Cross-Border Data Flows*, US Department of Commerce, September 2016 (1).
[321] Tania Voon, "Exploring the Meaning of Trade Restrictiveness in the WTO", *World Trade Review* Vol. 14 No. 3 (2015): 451, 456.
[322] WTO Appellate Body Report, *US – Gambling*, 308; WTO Appellate Body Report, *China – Publications and Audiovisual Products*, 326- 327; WTO Appellate Body Report, *EC – Seal Products,* 5.279.
[323] WTO Appellate Body Report, *Brazil – Retreaded Tyres,* 156; WTO Appellate Body Report, *China – Publications and Audiovisual Products,* 246.
[324] Commission Implementing Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided By the EU-U.S. Privacy Shield, *Decision C(2016) 4176 final*, July 12, 2016, ('EU−US Privacy Shield').

trust the reliability of those mechanisms, arguing that they provide insufficient level of protection.[325]

In these cases, the convening authorities, Panels or Appellate Body, can declare the alternatives not adequate and impractical, and consequently they could find such data restrictive measures justified under GATS Article XIV(c)(ii).[326]

3.2.1.2. Compliance with GATS Article XIV Chapeau

In parallel to Article XX GATT, the exception clause for trade in services also knows an introductory provision (Chapeau) introducing an additional restriction for the justification of a national measure to be considered to satisfy the exemption clause.

Indeed, once having assessed that a privacy-related data-restrictive measure satisfies the requirements of GATS Article XIV, it has to be consistent also with the chapeau of GATS Article XIV, which states that "Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures".[327]

WTO Panels have to analyse how the measures are implemented and operationalised[328] to prevent abuses of the GATS Article XIV exceptions, and to make sure that those measures are implemented according to the "good faith" principle.[329]

For the assessment of the violation of GATS Article XIV Chapeau in "its actual or expected application", WTO Panels have to look at the "design, architecture and revealing structure of a measure".[330] Sometimes the examination is not revealing, and in that case their enquiry may rely also to factual evidences.[331]

---

[325] Chris Connolly et al, "Privacy self-regulation in crisis? TRUSTee's "deceptive" practices", *UNSW Law Research Paper, (*UNSW 2014): 2, 3.
[326] *Ibid.*
[327] General Agreement on Trade in Services, chapeau art. XIV.
[328] WTO Appellate Body Report, *US – Gasoline*, 22.
[329] WTO Appellate Body Report, *US – Shrimp,* 158.
[330] WTO Appellate Body Report, *EC – Seal Products,* 5.302.
[331] WTO Appellate Body Report, *China – Rare Earths,* 5.113.

For the application of the chapeau of GATS Article XIV to a privacy-related data-restrictive measure, Panels have to determine if "like conditions" prevail, or through the WTO Member which impose the privacy measure and the other exporting WTO Members, or in case a measure restricts competition favouring or discouraging some exporting Members and not others. For instance, members with a strong data protection legislation, are unlike those members that have weak privacy and data protection laws. To establish if the measure constitutes "arbitrary or unjustifiable discrimination" or "disguised restriction on trade", it could be useful to stare at the various aspects of the design, structure and implementation of that measure.[332] For example, if a domestic measure impedes foreign suppliers from commercial surveillance, but it does not do the same with domestic suppliers, then that measure can be considered "arbitrary or unjustifiable discrimination". A similar case happens when a domestic law allows local suppliers to exercise data analysis across their entire customer network and at the same time deprive suppliers of those benefits. In this case a 'disguised restriction on trade in services' is constituted.[333]

In conclusion, it can be held that even though measure restricting cross-border data flows, related to the right to privacy, can violate obligations under the GATS, they can be provisionally justified under GATS Article XIV. However, a legal test shall be conducted, regarding different factors: if the measure is efficient for the protection of privacy, how and to what extent does it impact the trade of services, if there are other possible alternatives with a lower impact on trade and economy, etc.[334]

This inquiry is necessary to try to balance the needs of the international trade, the economy, and the need to ensure internet privacy to consumers and companies.[335]

3.3 The obligations clauses under the GATS: an introduction

As already discussed, one of the main goals of the WTO is to promote freedom in trade among countries without any type of discrimination.

---

[332] WTO Appellate Body Report, *US – Shrimp,* 156; WTO Appellate Body Report, *EC – Seal Products* 5.302.

[333] Diane A. MacDonald and Christine M Streatfield, "Personal Data Privacy and the WTO" *Houston Journal of International Law,* Vol. 36 No. 3 (2014): 629, 648.

[334] *Ibid.*

[335] *Ibid.*

Indeed, discrimination is the major factor which distorts the market, and consequently the fair trade. For this reason, the WTO introduced into its Agreements some obligation clauses with the function to prevent and oppose discriminatory behaviours.[336]

The principle of non-discrimination is a key of WTO law and policy and this is also proved by the Preamble to the WTO Agreement, which states that "the elimination of discriminatory treatment in international trade relations' is identified as one of the two main means by which the objectives of the WTO may be attained".[337]

In the following paragraphs there will be an analysis of the obligation clauses included in the GATS Agreement, which have the precise scope to favour the regulation of trade.

The Most-Favoured-Nation (MFN) Treatment obligation and the National Treatment obligation are the most important non-discrimination obligation clauses of the WTO legislative framework.[338]

To anticipate what will be the focus of the next sections, it can be now highlighted that the MFN treatment obligation clause concerns the favour of some countries over others in commercial decisions. The function of the clause is to prohibit the discrimination of a country between and among other countries.

The National Treatment obligation clause, instead, concerns the situation in which a country prefers and favours itself over other countries. It intends to prohibit this selfish behaviour, promoting trade among countries.[339]

The other two obligation clauses object of this research are the Market Access and Domestic Regulation obligation clauses.

Preliminarily, it has to be noted that Members decide the sectors in which they want to assume obligations and then they list them in their schedules of commitments.

---

[336] Peter Van den Bosche and Warner Zdouc, The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017)

[337] WTO Agreement, *Preamble*.

[338] Peter Van den Bosche and Warner Zdouc, The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017)

[339] Ibid.

However, limitations may be provided to commitments in order to have the right to operate measures inconsistent with full market access.[340]

The market access provisions of GATS cover six types of restrictions that must not be retained in the absence of limitations. The restrictions concern: the number of service suppliers, the value of service transactions or assets, the number of operations or quantity of output, the number of natural persons supplying a service, the type of legal entity or joint venture, the participation of foreign capital.

Regarding the last obligation clause in question, GATS makes an explicit distinction between domestic regulation and measures subjected to trade liberalization. It clearly ensures the right of Members to enforce domestic policy objectives through regulation, while promoting the scope of progressive liberalization, through the expansion and the improvement of existing commitments on market access and national treatment.

WTO recognises that effective regulation is a pre-condition for liberalization to produce the wanted efficiency gains without sacrificing quality or other policy objectives. Therefore, on the other side, it may be necessary to ensure that the advantages of the liberalization are not made useless by ineffective or inconsistent regulation.[341]

Some of the sectors in which Members can benefit from the Domestic Regulation obligation clause to pursue their policy objects are: consumer protection, labor market integration of disadvantaged persons, reduction of environmental impacts and other externalities, economic stability, avoidance of market dominance practices and anti-competitive conduct, prevention of tax evasion, fraud, etc.[342]

3.3.1. Most Favoured Nation Treatment obligation clause

In cases in which WTO members transfer their personal data exclusively to some other WTO members, they may violate the GATS non-discrimination obligations, since it can happen that certain data protection authorities require external suppliers to register their operations on personal data domestically, but these requirements could constitute an

[340] WTO, *GATS Basic Purpose and Concepts*, https://www.wto.org/english/tratop_e/serv_e/cbt_course_e/c1s7p1_e.htm (accessed January 19, 2021).
[341] Ibid.
[342] Ibid.

obstacle for smaller entrepreneurs and can result in a barrier for the access to such markets.[343]

WTO members have the duty to "accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country".[344] If the State fails to do so, it consequently violates the "most-favoured-nation treatment clause" under GATS Article II.

Only if "such a measure is listed in, and meets the conditions of, the Annex on Article II Exemptions[345]", Article II:1 GATS does not apply.[346]

When facing a data restrictive measure related to privacy, according to GATS, a three-requirement test has to be done.

First of all, it has to be examined, if the restrictive measure is covered under member's exemptions under GATS art II; then, whether the measure affects "like" digital services and service suppliers belonging to more than one different member, and third, if in the measure there is the provision of a less favourable treatment to "like" services and suppliers of two different members.

This test has to be carried out to establish the degree of fair competition between different services and service suppliers.[347]

The right to privacy comes into play when the trade assesses likeness of service and service suppliers to determine consumer preferences. For instance, consumers may distinguish between services with secure encryption and services without encryption or with a weak one.[348]

---

[343] UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development,* New York and Geneva 2016: 20.

[344] General Agreement on Trade in Services, art II:1.

[345] Annex on Article II Exemptions: "The agreed lists of exemptions under paragraph 2 of Article II appear as part of this Annex in the treaty copy of the WTO Agreement". Some of those are, for example, the preferential treatment for trade in frontier areas or the prudential carveaut in the area of financial services.

[346] General Agreement on Trade in Services, art II:2.

[347] WTO Appellate Body Report, *Canada – Autos,* 181; WTO AB Report, *Argentina – Financial Services,* 6.25, 6.26, 6.30- 6.32; WTO Panel Report, *EC – Bananas III* (Ecuador), 7.32; Won-Mog Choi, *Like Products in International Trade Law,* (Oxford University Press, 2003).

[348] WTO Appellate Body Report, *Argentina – Financial Services* 6.30, 6.38-6.45. Svetlana Yakovleva, "Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"?", *World Trade Review,* Vol. 17 No. 3 (2018): 477, 491-2.

In this case, if a WTO Panel is established, it could refer to the evidence provided by the parties on market competition, taking into account consumer surveys.

It can happen also that privacy preferences result in non-privacy competition, which happens in the case of countries where the sensitivity to privacy is very high, such as the European Union.[349]

The main problem is that consumers often are not sufficiently aware of the different privacy levels of the various digital services.[350] Without consumer preferences, the differences in privacy levels of digital services are not as necessary in determining likeness of services or service suppliers. For instance, encrypted social media and chat services, like "Viber" and unencrypted ones like "WeChat", are provided for almost the same functions. So, they are considered "like" services and there are not evident differences in consumer preferences.[351]

The "no less favourable treatment" requirement provided by GATS art II:1 refers to both de jure and de facto discrimination through like services and service suppliers.[352]

The test mentioned above investigates whether the restrictive measure in question results in the creation of different competitive conditions for like services and service suppliers of at least two WTO members. Thus, the assessment of less favourable treatment is not necessary to determine the legislative framework lying behind the discrimination. For instance, in case a member State bans "WeChat" (Chinese service supplier), because it is an unencrypted chat service, but does not do the same with "Viber" (Luxemburg service supplier), the ban in question is likely to violate GATS art II:1.[353]

---

[349] Mira Burri, "Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer" in *New Developments in Competition Behavioural Law and Economics* eds. Klaus Mathis and Avishalom Tor, (Springer, 2018): 241, 255.

[350] William Drake and Kalypso Nicholaidis, "Global Electronic Commerce and the General Agreement on Trade in Services: The "Millennium Round" and Beyond" in *GATS 2000: New Directions in Services Trade Liberalization,* eds. Pierre Sauve and Robert M Stern, *Liberalization* (The Brookings Institution, 2000): 399, 423.

[351] WTO Appellate Body Report, *Argentina – Financial Services,* 6.25; Katherine Connolly, "Finding Space for Regulatory Autonomy in GATS Article XVII after *EC – Seals:* Public Services and the "Likeness" of Public and Private Service Providers", *Legal Issues of Economic Integration* Vol. 42 No.1 (2015): 57, 61.

[352] WTO Appellate Body Report, *EC-Bananas III,* 231, 233-234; WTO Appellate Body Report, *Canada – Autos,* 78; WTO Panel Report, *EC- Bananas III,* 7.303.

[353] WTO Appellate Body Report, *Argentina – Financial Services*, 6.151, 6.124-6.126.

3.3.2 The National Treatment obligation clause

The National Treatment obligation clause is provided by Article XVII of GATS, according to " In the sectors inscribed in its Schedule, and subject to any conditions and qualifications set out therein, each Member shall accord to services and service suppliers of any other Member, in respect of all measures affecting the supply of services, treatment no less favourable than that it accords to its own like services and service suppliers. 2. A Member may meet the requirement of paragraph 1 by according to services and service suppliers of any other Member, either formally identical treatment or formally different treatment to that it accords to its own like services and service suppliers".

In order to determine if a measure falls into the scope of Article XVII, the members' schedules have to be analyzed and it should be identified whether a member has agreed to any commitments regarding the sectors and modes of delivery. That is, concerning the privacy-related data-restrictive measures, in its schedules on national treatment. Then, a specific test (such as the MFN test explained above) has to be carried out to assess likeness of foreign and domestic services and service suppliers.

The last step consists in establishing if the less favourable treatment has been conferred to external services or service suppliers in accordance to the privacy-related data-restrictive measure.

In doing so, WTO panels may consider if the measure provides additional expenses for suppliers from abroad in the domestic market and affects competition, or if it provokes advantages to domestic services or service suppliers in terms of costs, or if it causes both the results. For instance, data localisation mostly benefits local service suppliers because they are more likely to administer and manage local servers than service suppliers from abroad. Thus, foreign suppliers would need to create and own new servers, creating competition issues for other foreign services and service suppliers and/or favouring domestic ones. If these types of data localisation measures are issued in sectors where members have agreed national treatment commitments in their schedule, there would be a violation of GATS art XVII.[354]

Moreover, the WTO Panel in China – Electronic Payment Services noted that, while the scope of the market access obligation under Article XVI:2 of the GATS "applies

[354] Nellie Munin, *Legal Guide to GATS,* (Wolters Kluwers, 2010): 159.

to six carefully defined categories of measures of a mainly quantitative nature", the scope of the national treatment obligation under Article XVII extends generally to "all measures affecting the supply of services"[355].

3.3.3. Market Access obligation clause and Domestic Regulation obligation clause

According to GATS Article XVI:2, market access obligation provides that a member must have inscribed commitments on market access in sectors covered by the measure.

The under examined measure should fall under at least one of the paragraphs of GATS Article XIV:2, providing market access quantitative and qualitative restrictions.

A Member may agree to full market access commitments for determined service sectors. Consequently, all privacy-related measures which ban cross-border data flows in that sector will decrease to zero for the foreign service suppliers. A complete restriction on market access resulting in a "zero quota" constitutes a violation of Article XVI of GATS.[356]

An example of the breach of GATS Article XVI can be found in a case related to China and with the imposition of the duty, for foreign cloud service suppliers, to partner with local companies.[357]

In particular, China has given full market access commitments on data processing and tabulation services and the WTO Panel found that these measures may violate GATS Article XVI(e), since they "restrict or require specific types of legal entity or joint venture" for the supply of cloud computing services in the country.[358]

WTO Members have to respect obligations about the implementation of domestic regulations. Article VI:1 of GATS provides that: "in sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application

[355] Panel Report, *China – Electronic Payment Services*, para. 7.652.
[356] WTO Appellate Body Report, US – Gambling, 238, 251, 373.
[357] US - China Business Council, "Optimizing Connectivity: Updated Recommendations to Improve China's Information Technology Environment" (February 2018) https://www.uschina.org/sites/default/files/uscbc_ict_recommendations_en.pdf (accessed August 5, 2020).
[358] *Ibid.*

affecting trade in services are administered in a reasonable, objective and impartial manner." [359]

The most accepted interpretation of the wording "measures of general application" is of measures that apply not only to some companies, but to all services and service suppliers. For example, a WTO member may have accepted, in its GATS schedule, full commitments on market access in a specific sector but may require data related to that sector to be managed and processed abroad only after obtaining an authorization or a certain license. Since this measure applies to all digital service suppliers which conduct their cross-border data operation in a specific field, this measure is considered of general application.[360]

According to Article VI:1 of GATS, such measure should be implemented fairly, or instance abolishing unnecessary administrative requirements to obtain authorizations and licenses.[361]

GATS Article VI:5 forbids WTO members from tightening licensing requirements or imposing technical standards, regarding the transfer of data, that would have the effect of "nullifying and impairing" the commitments that members have offered. This is even the case if they do not rely on objective criteria,[362] or "could not reasonably have been expected of that Member at the time the specific commitments in those sectors were made." [363]

Whenever an assessment regarding the reasonableness of the requirements or standards imposed by members is necessary, the WTO Panels may take into account international standards issued by "relevant international organizations"[364], such as the already mentioned standards deriving from the OECD Guidelines[365].

---

[359] General Agreement on Trade in Services, art. VI:1.

[360] US - China Business Council, "Optimizing Connectivity: Updated Recommendations to Improve China's Information Technology Environment" (February 2018) https://www.uschina.org/sites/default/files/uscbc_ict_recommendations_en.pdf (accessed August 5, 2020).

[361] *Ibid.*

[362] General Agreement on Trade in Services, art VI:5(a)(i); General Agreement on Trade in Services, art VI:4.

[363] General Agreement on Trade in Services, art VI:5(a)(ii).

[364] General Agreement on Trade in Services, art. VI.5(b).

[365] Christopher Kuner, "The European Union and the Search for an International Data Protection Framework" *Groningen Journal of International Law* Vol. 2 No. 2 (2014): 55, 59-60.

However, according to GATS Article VI:5, members are free to choose the technical standards to refer to in order to implement their domestic privacy laws.[366]

Regarding the right to privacy and data protection, members can decide to follow two different approaches: the one called "geographical approach", which operates by reducing data transfer across borders, for the activities of digital service suppliers; or the "accountability-based approach", which makes organizations liable for data processing, no matter where they operate.[367]

The "geographical approach" often contains some burdensome requirements on digital service suppliers operating in cross-border data management. Indeed, even when digital service suppliers decide to refer to company technical standards and best practices in their global data processing management, they may require further authorisations and/or licences to make the transfer of data possible to their foreign servers. Since no consensus, on the relevant standards on privacy and data protection, has been reached by WTO Members, GATS Article VI has not strong potential in the addressment of those requirements. Notwithstanding the fact that to obtain those licences is likely to be unnecessary.[368]

[366] Rolf H Weber, "Regulatory Autonomy and Privacy Standards under the GATS" *Asian Journal of WTO and International Health Law & Policy* Vol. 7 (2012): 25, 37.
[367] *Ibid* n. 2, 29-30.
[368] *Ibid.*

CHAPTER III - Case Study: The application of GATS regime on GDPR Data Restrictive Provisions

1. Cross-Border Data Flows Restrictions under the GDPR

As already mentioned in the first chapter of the thesis, the General Data Protection Regulation (GDPR) entered into force in May 2018, repealing the Directive 95/46/EC. Since then, it has become the most important regulation in the European legal framework regarding data protection and it stands as a role model for the adoption of data-related provisions around the world.

The European Union adopted the GDPR to pursue the policy objective of the promotion of the right to privacy of all the Union's citizens, and also to allow a free but controlled personal data flow in the EU.

It intends to conciliate these two purposes without prejudice of individuals' fundamental rights and freedoms, since it is designed to avoid the unlawful and unfair processing of data. It follows "specified, explicit and legitimate purposes" guaranteeing the security and accuracy of the information and ensuring the identification of data when it is needed. It also provides that people are guaranteed the right to have their personal information deleted, for example, when the data are not useful anymore or when it is not given a specific consent upon their processing by the data subject.[369]

The regulation of cross-border data flows is a primary concern of the GDPR. Ensured by many dispositions, the legitimate and safe transfer of personal data finds its broader and most effective protection in the provision of the "adequacy mechanism". This strategic foresight has the function of restricting trade if the non-EU countries, with whom a European one is doing business, are unable to ensure an adequate grade of data protection comparable to that guaranteed by the European Union.[370]

---

[369] General Data Protection Regulation, Article 5.1.

[370] General Data Protection Regulation Preamble (104); General Data Protection Regulation, Article 45.1 "A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation."

In particular, the Regulation, to preserve the level of protection of data ensured in the EU, establishes that: "a transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation."[371]

Transfers on the basis on an adequacy decision are regulated by Article 45 of the GDPR, according to which, the standards to compare the degree of privacy safeguards are set by the European Commission, which issues official adequacy decisions and states about the compliance of third parties with privacy protection levels.[372]

To compare these standards, a substantive evaluation is done taking into account how the legislation upon data protection is developed abroad and how it should be managed according to the EU system.

For the assessment of the proper protection level that has to be ensured, various criteria have to be looked at. For example, the nature of data could be analysed, because taking into account the difference between sensitive and non-sensitive data may have an important impact on the degree of protection needed.[373] Furthermore, the Commission shall take into account the rule of law and the protection of fundamental human rights, data protection rules and the implementation of such legislation. It has also to have regard to the presence or not of an independent supervisory authority establishing its functioning. Also, it has to look at the international commitments signed by the third country or international organization under exam.[374]

Then, the Commission, after having established the adequacy of the level of protection, may decide, by means of implementing act, that the third country, the territory or one or more specified sectors within a third country, or the international organisation which have been examined, ensures an adequate level of protection within the meaning of paragraph 2 of the Article 45. Furthermore, the implementing act has to provide for a

[371] General Data Protection Regulation, Article 45.
[372] Rolf H. Weber, "Transborder data transfer: concepts, regulatory approaches and new legislative initiatives", *International Data Privacy Law*, Vol.3, Issue 2, May 2013: 117-130.
[373] *Ibid.*
[374] General Data Protection Regulation, Article 45.2.

mechanism for a periodic review, which has to take into account the relevant developments in the third country or international organisation.[375]

According to the paragraph 5 of Article 45, if the Commission notices that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of the same Article, to the extent necessary, repeal, amend or suspend the adequacy decision issued in accordance with paragraph 3 of Article 45, without retro-active effect.[376] Only under justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3) GDPR (the so-called "Committee Procedure").

The process of the adoption of an adequacy decision includes the proposal from the European Commission, an opinion of the European Data Protection Board, the approval from representatives of EU countries and the adoption of the decision by the European Commission. However, the European Parliament and the Council may demand, in any moment, the European Commission to maintain, amend or withdraw the adequacy decision if its act goes beyond the implementing powers provided for in the Regulation.[377]

However, GDPR recognizes the possibility, under specific circumstances, not to restrict trade between a EU country and a non-EU one which has not reached a successful outcome under the adequacy mechanism.

For example, it can happen when digital service suppliers take charge of ensuring "appropriate safeguards" under the GDPR without specific approval by a supervisory authority: these solutions involve the adoption of any legally binding instruments between public authorities or institutions, the enforcement of binding corporate rules (BCRs), the adoption of standard data protection clauses approved by the EU Commission (SCCs), the use of certification mechanism through which digital service suppliers guarantee their compliance to the GDPR, etc.[378]

---

[375] General Data Protection Regulation, Article 45.3.

[376] Article 45 para 5.

[377]European Commission, "Adequacy Decisions, how the EU determines if a non-EU country has an adequate level of data protection", available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed August 2020).

[378] General Data Protection Regulation, Article 46.3.

Even without the adoption of "appropriate safeguards", digital service suppliers can still pursue the data transfer. The transfer of personal information of residents outside EU can be performed under the condition that the data owner must be informed of all possible risks and they must be assumed by this owner.

If the public interests or necessities for the performance of a contract require so, or for the protection of crucial interests of the data subject, the approval of supervisory authority is not binding.[379]

2. Assessment of compliance of GDPR Cross-border data flows restrictions with GATS regime on obligations: an introduction

This research has already analysed, in the first chapter, the absence of an international legislative framework regulating cross-border data flows. The WTO has not succeeded in the creation of recognized and shared treaties up to the last digital developments yet.

Although WTO Members have not given a universal definition of legitimate regulation of cross-border data flows, not qualifying the features of "trade distortion" neither,[380] in the WTO legal framework, numerous agreements are related to digital trade.[381] Furthermore, the WTO Dispute Settlement Body has at least qualified the object in question stating that the GATS applies to digital services[382], as observed in the previous chapter.

In this chapter, it will be analyzed the consistency of GDPR data-related provisions with GATS commitments under the obligations' regime.

2.1 Schedules of Commitments

[379] General Data Protection Regulation, Article 49.

[380] Susan A. Aaronson, Patrick Leblond, "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO", *Journal of International Economic Law* Vol. 21 No. 2, Oxford University Press (2018): 246.

[381] World Trade Organization, *Ministerial Declaration on Trade in Information Technology Products*, December 13, 1996.

[382] WTO DSB, Appellate Body Report, *Antigua and Barbuda v. United States, US-Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, of 7 April 2005, case no. ds285: 6.370; *United States v. China*, cit.: 363-365.

By examining the relationships between the GDPR and the GATS, a mention to the Schedules of Commitments has to be made beforehand.

GATS commitments must be read along with the EU's Schedules of Commitments. For instance, GATS commitments regarding market access or national treatment obligations rely on positive lists. According to the positive lists' procedure, WTO Members can undertake commitments on those sectors only if they are involved in their Schedules of Commitments.[383]

The structure of the Schedules of Commitments is defined by the WTO Service Sector Classification List[384], although the sectors of personal data processing and those regarding the privacy law are not included in this list.

Consequently, WTO Members cannot refrain from accessing the commitments by referring to the "positive list" approach. Furthermore, the processing of personal data is performed in the context of the supply of services in sectors, which are provided in commitments' schedules.[385]

Specifically, the EU undertook numerous commitments on the supply of services, such as computer[386] and financial services[387], which automatically includes the transfer and the management of personal data.[388]

The interpretation of the Schedules of Commitments may be demanding. In solving the issues, the WTO adjudicating authorities may come to different interpretations from those intended by WTO Members' when undertaking a commitment.[389]

---

[383] EU Commission, Services and investment in EU trade deals: Using "positive" and "negative" lists, April 2016, <http://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154427.pdf> (accessed August 10, 2020).
[384] World Trade Organization, *Services Sector Classification List*, MTN.GNS/W/120, July 10, 1991; Rolf H. Weber and Mira Burri, *Classification of Services in the Digital Economy*, Zurich: Schulthess, 2012.
[385] Kristina Irion, Svetlana Yakovleva and Marija Bartl, "Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements", *independent study commissioned by BEUC et al*., (Amsterdam: Institute for Information Law (IViR), July 13, 2016).
[386] General Agreement on Trade in Services, "EU Schedule of Specific Commitments", GATS/SC/31 April 15, 1994, s. 1.II. B c), d) and e).
[387] General Agreement on Trade in Services, "EU Schedule of Specific Commitments Supplement", 4 Revision, GATS/SC/31/Suppl.4/Rev.1, November 18, 1999.
[388] Kristina Irion, Svetlana Yakovleva and Marija Bartl, "Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements", *independent study commissioned by BEUC et al*., (Amsterdam: Institute for Information Law (IViR), July 13, 2016).
[389] *Ibid.*

2.2. The Most-Favoured-Nation Treatment (MFN) obligation clause

The first GATS obligation under analysis is the one related to the Most-Favoured-Nation Treatment (MFN).

More specifically, the subject of this research is the consistency of GDPR provisions regarding the adequacy mechanism and the EU-US Shield with the Most-Favoured-Nation Treatment obligation provided by GATS art II.

To establish if the EU adequacy mechanism may result in a breach of the MFN obligation, it is necessary to look at the nature of the EU Commission's adequacy decisions.

Indeed, to be consistent with GATS art II, it has to be stated that the different treatment, which results in the adequacy decisions only for some countries, is a necessary consequence of the determined likeness of the services at stake and the presence of a less favourable treatment. This last one has to be considered to the extent that it provokes a distortion of competition, favouring exclusively one country's services.[390]

Firstly, it must be remembered that one of the main purposes of the MFN obligation is to guarantee the same chances to supply "like" services, creating a fair environment for the WTO Members trading partners.[391]

WTO adjudicating bodies regard "like" services to those which can compete with each other. Although there is not an official list of "like" services, the likeness should be determined case by case.[392]

The same adjudicating bodies, in the application of MFN treatment, state that there is not a less favourable treatment when a measure "modifies the conditions of competition to the detriment of like services or service suppliers of any other Member."[393]

As already noted, according to the WTO Appellate Body, a violation of the MFN obligation can be the result of a *de jure* or a *de facto* differential treatment.[394] At this

---

[390] General Agreement on Trade in Services, art. II:1; WTO DSB, Panel Report, *Panama v. Argentina, Argentina-Measures Relating to Trade in Goods and Services*, September 30, 2015, case no. ds453: 7.147-7.149.

[391] WTO Appellate Body Report, *EC – Bananas III*, fn. 104: 234.

[392] WTO Appellate Body Report, *Argentina – Measures relating to trade in Goods and Services*, fn.104: para. 6.3.4.

[393] *Ibid*. paras 6.29f.

[394] WTO Appellate Body Report, *EC – Bananas III.*

point, providers who obtained an adequacy decision are more encouraged in business as they can take advantage of the right to freely transfer data from and to the EU. Services and service suppliers from countries which do not obtain that decision, instead, cannot do so.[395]

The adequacy decision mechanism thus can cause a *prima facie* most favourable treatment to those who prove to satisfy the requirement of the equivalent data protection level guaranteed, even if this behaviour does not result directly as discriminatory.

However, as mentioned above, even without a positive adequacy decision, digital service suppliers can conduct business with EU Members by making use of safeguards, such as BCRs and SCCs, even it should be noted that those safeguard mechanisms are expensive and of difficult implementation in terms of both time and technical procedures. This means that not all countries or companies can afford such expensive and burdensome solutions.[396]

Therefore, this disparity of provisions in terms of guarantees offered can lead to adequacy decisions which may be declared in violation of the MFN commitment by the WTO adjudicating bodies.[397]

The result is that service suppliers which are outside the European Union and have not the means to afford the proper instruments to adequate their safeguard mechanisms to the EU standards, find themselves automatically outside the business.

Indeed, if their privacy mechanisms are not in compliance with the EU mechanisms, they cannot have access to the users' data of that market, and this means that they cannot operate in that market. Thus, it would be useful a system which could support these suppliers, technically and economically, in the implementation of privacy related measures not to remain excluded from the global business conduct.

---

[395] Aaditya Mattoo and Joshua P Meltzer, "International Data Flows and Privacy the Conflict and Its Resolution"*, Journal of International Economic Law,* Vol. 21 (2018): 171, 777-9.

[396] *Ibid.*

[397] WTO Panel Report *Ecuador, Guatemala Honduras, Mexico and United States v. European Communities*, cit., paras 7.349-7.353; WTO Appellate Body Report *Panama v. Argentina*, cit., paras 6.5-6.8.

2.3. Market Access and National Treatment obligations clauses

The GATS articles XVI, about Market Access, and XVII, about National Treatment, provide obligations which apply in line to the Member States' Schedule of Commitments on service sectors[398], as seen in the previous chapter.

Particularly, the EU Commitment for the processing of personal data consists of avoiding restrictions regarding national treatment and market access.[399]

According to GATS art. XVII:1, it is forbidden to provide a less favourable treatment than the one agreed to national like services and service suppliers, similar services, and service suppliers of other WTO Members.[400]

Additionally, the second paragraph clarifies that the commitment on the national treatment provided by the GATS refers to both "formally identical" and "formally different" treatments accorded to like services and service suppliers between two or more WTO Members.[401] The third paragraph of the same article provides that there is a less favourable treatment whenever the "formally identical" or "formally different" treatment distorts fair competition.[402]

From the EU perspective, following the GDPR adequacy mechanism, it can be distinguished between third countries which successfully obtained an adequacy decision and third countries which did not.

The first group of countries, once established the EU data protection levels, has the opportunity to freely trade and manage data from and to the EU. The second group cannot do so.[403]

---

[398] Stefano Saluzzo, *"*Cross Border Data Flows and International Trade Law. The Relationship Between EU Data Protection Law and the GATS*", Diritto del Commercio Internazionale,* Vol. 4 (2017).

[399] European Communities and their Member States - *Schedule of Specific Commitments*, GATS/SC/31, April 15, 1994: 32.

[400] General Agreement on Trade in Services, Article XVII.

[401] General Agreement on Trade in Services, Article XVII:2.

[402] General Agreement on Trade in Services, Article XVII:3.

[403] European Commission, "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection", *ec.europa.eu*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy decisions_en#:~:text=How%20the%20EU%20determines%20if,adequate%20level%20of%20data%20protection.&text=The%20European%20Commission%20has%20the,adequate%20level%20of%20data%20protection. (accessed August 10, 2020).

Since not many countries manage to reach those levels of compliance, the majority of non-EU countries is excluded from trade within the EU. The risk is the creation of a huge gap between non-EU countries and EU ones whose legislations comply with the GDPR.[404]

A debate has been raised and the compliance system, shaped by the GDPR, has been accused of modifying "the conditions of competition in favour of services based in EU/EEA".[405] Certainly, it has been argued that the non-EU suppliers complying with GDPR requirements takes a much more effort than the ones performed by domestic suppliers.[406]

Thus, in this case, it would be up to the EU to demonstrate that the level required by the GDPR is the most appropriate one for the achievement of a fair competitive environment.[407]

WTO adjudicating bodies, when deciding matters of this nature, would proceed to a case-by-case analysis, first, on the likeness of the services and, then, on the presence of an effective different treatment between EU and non-EU suppliers; finally, it should assess the consequences of the different treatment for the competition environment.[408]

Regarding Market Access obligation clause, GATS article XVI:1 states that WTO Members have to grant treatments on services and service suppliers of other Members no less favourable than "the terms, limitations and conditions agreed and specified" in their Schedules.[409]

---

[404] *Ibid.*

[405] Kristina Irion, Svetlana Yakovleva and Marija Bartl, "Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements", *independent study commissioned by BEUC et al.,* (Amsterdam: Institute for Information Law (IViR), July 13, 2016).

[406] Paul de Hert and Michal Czerniawski, "Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context", *International Data Privacy Law* Vol. 6 Issue 3, (August 2016); Merlin Gömann, "The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement", *Common Market Law Review*, (2017).

[407] Svetlana Yakovleva and Kristina Irion, "The Best of Both Worlds – Free Trade in Services and EU Law on Privacy and Data Protection", *European Data Protection Law Review* (2016)*:* 204; Gilles Muller, "De Facto Discrimination under GATS National Treatment: Has the Genie of Trade Liberalization Been Let Out of the Bottle?", *Legal Issues of Economic Integration*, (2017): 166-172.

[408] Federica Velli, "The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements", *European Papers* Vol. 4 No. 3 (European Forum, December 9, 2019).

[409] General Agreement on Trade in Services, Article XVI.1.

At the second paragraph, the article lists series of market access barriers that results in quantitative restrictions, such as the limitations on the number of service suppliers, limitations on the total value of service transactions or of service operations, etc.[410]

The provision of these restrictions is unlawful unless the Members have inserted those in their Schedules. The EU does not list any of those restrictions in its Commitments' Schedules.[411].

> As analyzed in the previous chapter, the WTO Appellate Body, in deciding the US-Gambling case, established that there was a breach of the principle of market access due to a zero quota ban on the online gambling services' remote supply. Indeed, it noted that, on sectors included in commitment schedules, the issue of service supplies prohibiting measures regarding those sectors may result in a limitation according to GATS article XVI:2(c).

The restriction can also result in a violation of GATS Article XVI:2(a), because it can amount to a reduction of service suppliers' numbers in the form of numerical quotas.[412]

By applying the GDPR, there is no risk to find a "zero quota" violating GATS art XVI.

Even if the adequacy system restrictions may lead to the prohibition for service suppliers operating in the data related sector from conducting their businesses, which constitutes a zero-quota limitation for entering into the EU services market, and breaching GATS Article XVI:2(a) and (c),[413] the Regulation contains the provision of further options reserved to those do not satisfy the adequacy system's requirements, like the data subject express consent or the corporate binding rules.[414]

---

[410] General Agreement on Trade in Services, Article XVI.2.

[411] Panagiotis Delimatsis, Martin Molinuevo, "Article XVI GATS: Market Access", *Max Planck Commentaries on World Trade Law, WTO- Trade in Services,* in Rüdiger Wolfrum, Peter-Tobias Stoll, Clemens Feinäugle, eds., Vol 6 (Leiden/Boston: Martinus Nijhoff Publishers, 2008). Available at SSRN: https://ssrn.com/abstract=1280219.

[412] WTO Appellate Body, *US-Gambling*, cit., para. 252.

[413] Carla L. Reyes, "WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive", *Melbourne Journal of International Law*, pp 22-23.

[414] Svetlana Yakovleva and Kristina Irion, "The Best of Both Worlds – Free Trade in Services and EU Law on Privacy and Data Protection", *European Data Protection Law Review*, 204; Gilles Muller, "De Facto Discrimination under GATS National Treatment: Has the Genie of Trade Liberalization Been Let Out of

In this sense, data transfer measures are not qualified as zero-quota restrictions, and they do not result in quantitative restrictions under the scope of market access' obligations neither.[415]

Certainly, the different treatment for the suppliers resulting from the application of the adequacy mechanism can result in a *de facto* discriminating behaviour, but it does not regard the scope of market access commitments.[416]

2.4. Domestic Regulation obligations and the Mutual Recognition Principle

According to the GATS obligation on domestic regulations, WTO Members must guarantee the reasonableness, objectiveness and impartiality in the administration of all the measures of general application dealing with trade in services.[417]

Thus, WTO Members are entitled to issue domestic regulations affecting trade in services if they fulfil the provision of the Article VI:1 of the GATS.

As a guarantee to the service suppliers, the second paragraph of GATS Article VI requires WTO Members to provide judicial, arbitral, or administrative tribunals or procedures for reviewing the enacted measures dealing with trade in services.[418]

The purpose of this article is to prevent national measures from being applied in an inconsistent manner with WTO principles of predictability and fair trade, trying not to compromise the foreign service suppliers' operations. The provision arises concerns about the application, because also an objectively lawful provision may breach the principles of consistency and predictability if it is not applied in line with the entire legislative framework.[419]

---

the Bottle?", Legal Issues of Economic Integration, (2017); WTO, Panel Report*, US - Gambling*, cit., para. 3.141 et seq.

[415] Panagiotis Delimatsis, Martin Molinuevo, "Article XVI GATS: Market Access", *Max Planck Commentaries on World Trade Law, WTO- Trade in Services,* in Rüdiger Wolfrum, Peter-Tobias Stoll, Clemens Feinäugle, eds., Vol 6 (Leiden/Boston: Martinus Nijhoff Publishers, 2008). Available at SSRN: https://ssrn.com/abstract=1280219.

[416] Stefano Saluzzo, *"Cross Border Data Flows and International Trade Law. The Relationship Between EU Data Protection Law and the GATS", Diritto del Commercio Internazionale,* Vol. 4 (2017).

[417] General Agreement on Trade in Services, Article VI:1.

[418] General Agreement on Trade in Services, Article VI:2.

[419] Panagiotis Delimatsis, *International Trade in Services and Domestic Regulations, Necessity, Transparency and Regulatory Diversity,* International Economic Law, Oxford (Oxford, December 27, 2007).

Additionally, for the scope of Article VI, the enacted measure may also indirectly affect trade in services. Indeed, the provision covers measures issued to achieve public policy objectives too.[420] What is in the spotlight is not the content of the measure *per se,* but rather the efficiency of the domestic administrations.

Domestic regulations obligations can affect the administrative and judicial procedures carried out for the compliance to the adequacy principles by the EU Commission. Thus, the consistency of EU data transfer measures with GATS provisions is not under the scope of Article VI.

Indeed, Members' right to regulate did not prevent the inclusion in the GATS of provisions allowing for the minimisation of the trade restrictive effects of domestic regulation (not falling) within the scope of Articles XVI and XVII. Those rules are promoted in Article VI of the GATS, which contains: (a) some binding provisions; (b) a mandate for the development of multilateral disciplines; and (c) a mechanism for the provisional application of the main principles underlying the future disciplines.[421]

As the Commission benefits from the possibility of introducing and imposing certain requirements to non-EU countries to ensure a high grade of data privacy protection and fairness, its actions may lead to unpredictable procedures. Hereby, WTO Members can debate all the procedure under the "arbitrary application of domestic regulation's" legal basis. [422]

Other possible violations of the GDPR regime with GATS have been argued on the principle of mutual recognition, and especially regarding the application of the second and third paragraphs of GATS Article VII.

GATS Article VII:2 provides that when a WTO Member grants licenses or certifications to the service supplier of another WTO Member, it has to ensure the same

---

[420] Robert W. Hahn, *Reviving Regulatory Reform: A Global Perspective*, The AEI Press (Washington, D.C, 2000): 7; Panagiotis Delimatsis, *International Trade in Services and Domestic Regulations, Necessity, Transparency and Regulatory Diversity,* International Economic Law, Oxford (Oxford, December 27, 2007).

[421] Contra see Carla L. Reyes, "WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive", Melbourne Journal of International Law, pp. 18-20; criticized by Svetlana Yakovleva and Kristina Irion, "The Best of Both Worlds – Free Trade in Services and EU Law on Privacy and Data Protection", *European Data Protection Law Review*.

[422] Stefano Saluzzo, *"*Cross Border Data Flows and International Trade Law. The Relationship Between EU Data Protection Law and the GATS*", Diritto del Commercio Internazionale,* Vol. 4 (2017).

treatment and it has to "afford equal opportunities" for any other Member interested in the establishment of the same or "like" agreements.[423]

GATS Article VII:3 states that a WTO Member has to accord recognition not discriminating countries on the ground "of the application of its standards and criteria for the authorization, licensing or certification of service suppliers, or a disguised restriction on trade in services".[424]

In case of disputes about the violation of GATS article VII:3, it would be up to the third member state to demonstrate not only the consistency of its data legislative framework to the GDPR, but also the validity and/or the similarity of its regulatory framework compared to the US legislation on data protection.[425]

3. Assessment of compliance of GDPR Provisions with the GATS General Exceptions. GATS Article XIV(a) and Article XIV(c)

The WTO legislation provides a system of general exceptions to let WTO Members pursuing their policy objectives without resulting inconsistent with the Agreements' provisions.

More precisely, as seen in the previous chapter, GATS Article XIV allows Members to issue measures which may have negative effects on international trade in services, finding their justifications under different grounds.

Regarding the case of the inconsistency of GDPR provisions with the GATS, the EU provisions on the processing of data can find their justification under the GATS Article XIV(a), which supports the promotion of "public morals" and "public order".[426]

This provision has been interpreted by the WTO adjudicating bodies in a very broad way, to include all the shared values of all the actors having regards of the various social, economic, and cultural backgrounds.

[423] General Agreement on Trade in Services, Article VII:2.
[424] General Agreement on Trade in Services, Article VII:3.
[425] *Ibid.*
[426] General Agreement on Trade in Services, Article XIV(a).

Back to the EU case, the right to privacy and data protection has been considered a social and cultural value common to the whole Union.[427] Indeed, it is at the basis of all the community treaties, being promoted as a fundamental human right.[428]

As the violation of the right to privacy is a breach of a fundamental value, it can cause invaluable damages, such as identity fraud and cybercrimes, loss of confidentiality and discretion[429], and generally security breaches. Since all these violations aim to target the public order and the peoples' trust, the EU may invoke Article XIV(a) of the GATS to justify GDPR restrictive provisions towards non-EU countries.

According to the GDPR Preamble, the Regulation has the purpose to guarantee that the data protection measures adopted would meet the requirements and the principles of EU provisions in terms of data protection standards. For instance, not allowing the transfer of EU data to those third parties which do not comply with a certain level of data protection.[430]

Thus, the various systems provided by the EU, such as the adequacy mechanism and the EU-US Privacy Shield, have the function to create a uniform and necessary set of standards to promote the right to privacy and to protect the data of the EU citizens.[431]

Moreover, the EU can find a justification for its GDPR data restrictive measure under the GATS Article XIV(c)(ii) too.[432]

Resuming the statement of the article, it allows WTO Members to take data-related restrictive measures if they are: "(c) necessary to secure compliance with laws and regulations which are not inconsistent with the provisions of this Agreement including those relating to: […] (ii) the protection of the privacy of individuals in relation to the

[427] European Data Protection Supervisor, "Data Protection", available at <https://edps.europa.eu/data-protection_en> (accessed August 11, 2020).
[428] Charter of Fundamental Rights of the European Union, Article 8(1); Mira Burri and Rahel Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", *Journal of Information Policy,* Vol. 6 (2016): 479, 481.
[429] General Data Protection Regulation Preamble, [75].
[430] General Data Protection Regulation, Preamble.
[431] Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", *International Data Privacy Law* Vol.5 No.4 (2015): 235, 239-240.
[432] *Ibid.*

processing and dissemination of personal data and the protection of confidentiality of individual records and accounts".[433]

Observing the wording of the Article, GDPR data restrictive provisions may fall under its scope if the EU manages to prove that those provisions are essential to fulfil the standards and requirements contained in the Regulation.

The enactment of data restrictive measures by the EU prevents third countries to conduct processing operations on EU data operators in contrast with the principles of lawfulness, transparency, confidentiality, and security. All principles which are consistent with WTO legislation too.[434]

To establish if a GDPR data restrictive measure falls within the scope of GATS Article XIV, a two-tier test has to be conducted.

More precisely, the measure under analysis has to fall within at least one exception of the norm and it has not to be applied in a discriminatory way or arbitrary manner in case of like conditions between two or more countries.[435]

As already examined in the second chapter, the WTO Panels are in charge to qualify a provision as necessary or not comparing it with the requirements of GATS Article XIV.

In particular, it has to be assessed if the measure complies with the GATS' policy objectives through a weight and balance test of the values promoted by the Agreement. The WTO Panels' overview has to take also into account the impact of the data restrictive measure on the sectors of trade and it has also to consider possible alternative options which would less affect the international data flow and, consequently, the international trade of services.[436]

Regarding the assessment of the necessity of the EU data restrictive measures, it has been argued that the EU has issued more restrictive measures than those that would be necessary to ensure the data protection and the right to privacy of EU users and consumers.

---

[433] General Agreement on Trade in services, Article XIV(c)(ii): "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts".

[434] Panel Report, *Argentina - Financial Services,* 7.622 - 7.625.

[435] Stefano Saluzzo, *"*Cross Border Data Flows and International Trade Law. The Relationship Between EU Data Protection Law and the GATS*", Diritto del Commercio Internazionale,* Vol. 4 (2017).

[436] General Agreement on Trade and Services, Article XIV.

Indeed, it could have lowered the required standards of the adequacy mechanism or it could have reduced the data flow with non-compliant third countries to avoid a total interruption of transfers.[437]

Putting aside the speculations on what it would have been better to do or not, the first thing to assess, in order to determine the necessity of a measure, is its policy objectives.[438]

In the present analysis, the policy objective pursued is the right to privacy. As seen in the first chapter, the latter is considered a fundamental human right being promoted by numerous international conventions on human rights, having reached also a constitutional status in nature.[439]

The further step of the necessity test is to establish whether the restrictive measures actually help the objectives of protecting the privacy and promoting data protection as provided by the EU defined standards.

Measures restricting trade under the EU legislative framework, especially under the adequacy system, make sure that the level and the guarantee of the right to privacy and data protection are not only high, but also effective.

For this reason, it can be said that under the GATS Article XIV(c) the adequacy mechanism is necessary to achieve the EU policy objectives.[440]

The next step to assess the necessity of a data restrictive measure is in consideration of its impact on international trade, having regard to all sectors of the worldwide economy.

---

[437] Carla L. Reyes, "WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive", *Melbourne Journal of International Law*: 32-33; Christopher Kuner, "Developing an Adequate Legal Framework for International Data Transfers", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt eds., *Reinventing Data Protection*?, (Springer, 2009): 263 et seq.

[438] WTO Appellate Body, *Korea - Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, WT/DS161/AB/R and WT/DS169/AB/R, December 11, 2000: para. 161.

[439] International Covenant on Civil and Political Rights, Article 17; European Convention on Human Rights, Article 8; Rachel Harris and Gillian Moon, "GATT Article XX and Human Rights: What Do We Know form the First 20 Years", *Melbourne Journal of International Law*, (2015): p. 432 et seq.

[440] European Commission, "EU-US Privacy Shield: Second Review Shows Improvements but a Permanent Ombudsperson Should be Nominated by 28 February 2019" (Press Release, December 19, 2018) available at <http://europa.eu/rapid/press-release_IP-18-6818_en.htm>. (accessed August 11, 2020).

Since GDPR restrictive measures affect personal data flow, the impact on the restriction of trade is very significant.[441] It affects, mostly, the vulnerable actors of the economies, for example small business and enterprises which cannot afford the huge expenses in terms of cost and time that the implementation of rules needs, according to the EU standards.

Additionally, WTO adjudicating bodies have to determine whether an eventual alternative measure, less restrictive than the one in question, provided by the complainants, could be applied and it's effective in the achievement of the EU required level of privacy. For example, this can happen in case a complainant suggests protecting EU data through the imposition of specific barriers on digital service suppliers, such as technological requirements.[442]

The GDPR already has adopted the "privacy-by-design" procedure, to ensure the enforcement of "technical and organizational measures"[443]. Those measures have the function to provide that "the principles of data protection by design and data protection" are implemented in digital services "by default".[444]

However, it could be argued that DPR privacy-by-design requirement does not directly satisfy EU data protection standards. First, because EU data protection authorities are not able to accurately monitor the compliance of each digital service supplied within the EU standards.[445] Then, because of the lack of data protection international standards,[446] to determine whether a service respects the privacy-by-design requirements is an unpredictable process.[447]

---

[441] Erik van der Marel, Hosuk Lee-Makiyama, Matthias Bauer, "The Costs of Data Localisation: A Friendly Fire on Economic Recovery", *ECIPE Occasional Paper* 3/2014, ECIPE, May 2014**:** 6, 8.

[442] W. Kuan Hon, *Data Localization Laws and Policy,* (Cheltenham, UK; Northampton, MA, USA: Edward Elgar, 2017).

[443] General Data Protection Regulation, Article 25 (1).

[444] General Data Protection Regulation, Preamble [78]; General Data Protection Regulation, Article 25 (1).

[445] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, "Privacy and Data Protection by Design – from policy to engineering", *European Union Agency for Network and Information Security,* December 2014, www.enisa.europa.eu.

[446] Christopher Kuner, "Developing an Adequate Legal Framework for International Data Transfers", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt eds., Reinventing Data Protection?, (Springer, 2009): 263, 269.

[447] Fred H. Cate, Christopher Kuner, Dan Jerker B. Svantesson, Orla Lynskey, Christopher Millard, "The Language of Data Privacy Law (and How it Differs from Reality)", *International Data Privacy Law,* Vol.6 No.4 (2016): 259, 259; Lee A. Bygrave, "Hardwiring Privacy" in Roger Brownsford et al., eds., *The Oxford Handbook of Law, Regulation and Technology,* (Oxford University Press, 2017): 755, 759, 772.

Therefore, under GATS Article XIV, provisions like the privacy-by-design one are not regarded as possible alternatives. They are considered as just a fragment of the EU broad and "complex suite of measures" to promote the right to privacy and data protection.[448]

3.1 Assessment of compliance of the GDPR Compliance with GATS Article XIV Chapeau

As analyzed in the previous chapter, in order to be justified under GATS Article XIV, a data restrictive measure not only has to be declared as "necessary" for the achievement of the policy objectives of Article XIV, but it also has to be compliant with its *chapeau* too.

For being in compliance with the GATS Article XIV *chapeau*, three standards have to be fulfilled simultaneously. These requirements concern the arbitrary discrimination towards Members in presence of like conditions, the unjustified preference of a country in respect of another in the same context, and the causation of distorting effects on competition in the international trade context.[449]

All three standards have to be accomplished for the measure to fall within the scope of the GATS Article XIV *chapeau*. Thus, to access the effective compliance to the Regulation, a complete exam of the domestic measure and its implementation is necessary.[450]

However, the implementation of EU rules is not uniform, mainly due to the discretional power of the EU Commission. Certainly, there is no objective criteria according to which the Commission should agree on adequacy assessments to some countries instead of others. Numerous countries are still excluded from the system even if they have strong data protection legislation.[451]

---

[448] WTO, Appellate Body Report, *Brazil – Retreaded Tyres* [151],[211]; WTO, Panel Report, *China – Rare Earths* [7.186]; WTO, Panel Report, *Australia — Tobacco Plain Packaging (Indonesia)* [7.1384] – [7.1391].

[449] WTO, *Panel Report, US - Gambling* [6.581]; WTO, Appellate Body, *United States - Import Prohibition of Certain Shrimp and Shrimp Products (US - Shrimp)*, WT/DS58/AB/R, October 12, 1998: para. 150.

[450] Stefano Saluzzo, *"*Cross Border Data Flows and International Trade Law. The Relationship Between EU Data Protection Law and the GATS*", Diritto del Commercio Internazionale,* Vol. 4 (2017).

[451] Svetlana Yakovleva and Kristina Irion, "The Best of Both Worlds – Free Trade in Services and EU Law on Privacy and Data Protection", *European Data Protection Law Review,* 206.

In such cases of unpredictability also a justification for data restrictive measures based on GATS Article XIV seems quite hard to claim.[452]

As examined, the WTO system finds numerous challenges in the balance of the obligations provided by its legislative framework and the GDPR.

3.2 International Trade Law and EU Law: how to coexist and to cooperate

As it has been analysed through the thesis, one of the aims of international trade law is to encourage digital cross-border trade, and to do so, it is necessary to liberalize data flow; the European Union, on its side, tends to limit the transfer of personal data outside the European Economic Area through its data protection measures.

In order to ensure the fundamental rights to the protection of personal data promoted by Article 8 of the EU Charter of Fundamental Rights, all the rules governing the transfers of personal data outside the EEA shall ensure the protection of data at the same level in which it is guaranteed by the EU through the General Data Protection Regulation. Indeed, data protection must not be neither abandoned or undermined as they leave the EEA.

This state of things creates a tension between the scopes of the two systems: EU law allows cross-border data flows as long as the protection, in line with the EU Charter and domestic rules for such flows, is preserved; International trade law, instead, tolerates EU's restrictive measures on the transfer of personal data only if such restrictions respect the EU's international trade liberalization commitments including also allowable exceptions thereto.[453]

Though, both the systems provide EU exceptions which allow them to tolerate each other and to coexist. One of the first exceptions examined has been the Article XIV of the GATS, which has become a model for most of the provisions contained in the various international trade agreements.

To recall what has already been described through the thesis, this exception has the function to allow parties to an international trade agreement to undertake or to

---

[452] Stefano Saluzzo, *"Cross Border Data Flows And International Trade Law. The Relationship Between EU Data Protection Law and the GATS", Diritto del Commercio Internazionale,* Vol. 4 (2017).

[453] Svetlana Yakovleva, "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'", *Journal of World Investment & Trade* Vol. 21 (2020): 881–919.

maintain measures "necessary" for the protection of data, in the context of the collection and processing of data, to ensure the privacy of individuals, even if such protective measures infringe country's international trade commitments. In particular, Article 52(2) of the EU Charter, provides a "necessity test" which consists in determining whether the EU may limit fundamental rights or not on the basis of the protection of public general interest or to protect the rights and freedoms of others.

In the context of the application of the fundamental right to the protection of personal data promoted in Article 8 of the EU Charter, along with the obligation to liberalize international trade, Article XIV GATS enshrining the general exception for privacy and data protection and Article 52(1) establishing the derogation clause of the EU Charter are mutually exclusive.

By examining the clash between these two systems, it can be noticed that the trade "necessity test", which is the core of the GATS general exception, could be too limited to help EU's autonomy to uphold the GDPR framework for transfers of personal data. Consequently, the EU can be demanded by the WTO to align the rules on cross-border transfers of personal data in conformity to the international trade commitments and, potentially, it can be required to abandon the adequacy approach too.

From the point of view of the EU law, signing an international trade agreement or complying with provisions restricting any of the fundamental rights enshrined by the EU Charter is an exemption from the EU Charter and thus is subject to its Article 52(1). According to this provision, "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

As affirmed by the CJEU, the derogation clause applies to both internal and external legislative acts of the EU, such as international agreements. The CJEU declared the supremacy of the EU Charter over the EU's international agreements and definitely stated that the EU cannot sign nor implement, through a legislative act, international agreements that do not comply with the "necessity" test.

An instrument to declare that an international trade agreement is consistent with the EU's legislative framework is provided by Article 218(11) of the TFEU, which applies in the preliminary stage to its conclusion.

Specifically, due to this mechanism, the EU Member States, the European Parliament, the Council or the European Commission have the possibility to request to the CJEU for an opinion on the compatibility of a certain international agreement with the EU Treaties and the EU Charter. The result is that, if the CJEU pronounces the non-conformity of the agreement to the EU Treaties and/or Charter, such agreement cannot enter into force nor become binding until and unless it is modified and aligned to EU fundamental provisions.

A case in which this provision was applied, was the request of the European Parliament concerning the EU–Canada agreement on the transfer and processing of Passenger Name Record data, which transferred Europeans' personal data to Canada. In this emblematic ruling, having declared such provisions against the requirements of the derogation clause and of those of the EU Charter "necessity test", the CJEU stated that the agreement at stake could be signed only if revised in compliance to EU norms.

By now, it is CJEU settled case law that international agreements to be effective in the entire EU must be "entirely compatible with the Treaties and with the constitutional principles stemming therefrom",[454] and more precisely with the right to privacy personal data protection.[455]

However, this point needs to receive attention, because if the EU framework for personal data transfers were declared incompatible with a trade agreement, for instance for not respecting the requirements of the "necessity test" prescribed in the general exception, and consequently the EU needed to revise its laws to brought them in compliance with such agreement too meet the decision of a trade adjudicating body, this would be an exemption from the fundamental rights enshrined by Articles 7 and 8 of the EU Charter.

Thus, according to the CJEU's jurisprudence, it is necessary to determine the compliance to an international trade agreement (testing this latter under Article 52(1) of

[454] Court of Justice of the Euopean Union, *Opinion 1/15 (n 1).*

[455] Svetlana Yakovleva, "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'", *Journal of World Investment & Trade* Vol. 21 (2020): 881–919.

the EU Charter), before a decision of an international trade adjudicating body could be implemented.

To further deepen this argument, it should be noticed that international trade law's "necessity test", *per se* conceived as an exemption from the EU's fundamental right to privacy and the protection of personal data, is implausible to meet the EU Charter "necessity test", because the trade "necessity test", requires the EU to derogate from fundamental rights more than it could do under Article 52(1) of the EU Charter.[456]

Furthermore, from the jurisprudence of the CJEU, it can be derived that any measure of the EU which has the object of personal data processing, such as the collection, the use or transfer of individual information, is *per se* a restriction of the fundamental right to privacy and protection of personal data, no matter if such limitation can be justified under some exceptions or not. Therefore, such restrictive measure first of all, requires the assessment under Article 8(2) of the EU Charter, then, it requires also another assessment under the requirements of Article 52(1) of the EU Charter to be considered lawful.

To better understand the issues raised, it should be evidenced that, if on one side it is true that international trade agreements are binding on the EU, enough to form an "integral part" of its legal system, on the other side, in the hierarchy of sources of law, EU primary law prevails over the EU's international trade commitments. In addition, international trade agreements and decisions of international trade adjudicating bodies do not have direct effect within the EU system. However, under international law the EU has to act in good faith and this means that it has to fulfil its obligation under international trade law anyway, becoming liable if it fails to do so.[457]

To sum up, the collision between the two systems may not heal considering the WTO legal status within the EU.

---

[456] Charter of Fundamental Rights of the European Union, Article 52(1): "1.Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

[457] Svetlana Yakovleva, "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'", *Journal of World Investment & Trade* Vol. 21 (2020): 881–919.

Certainly, the EU tends not to recognise the direct effect of the WTO provisions, and not even the decisions of the WTO DSU.[458] This practice harms the enforcement of the GATS commitments in the EU legal system because it would find numerous obstacles which require more time and effort. This behaviour has a negative impact, also, on the reconciliation of apparently conflicting obligations through judicial interpretation and control.

Furthermore, the assessed "constitutional" nature of data protection restrictive measures, which legal basis are in articles 7 and 8 of the EU Charter of Fundamental Rights, may result in a means for the EU to get over its international trade-related obligations under the objective of the right to privacy and data protection.[459]

In conclusion, it could be said that a primary role, under this perspective, is played by the European Commission, which stands in a useful position to prevent that conflicts arise with WTO obligations. Moreover, as the executive body of the EU, the Commission has to be careful in dealing with the field of data transfers, and it always has to find itself in compliance with the principles of transparency and non-discrimination.[460]

Following its duties and WTO obligations and provisions on the implementation of its rules related to cross-border data flows, it may prevent arguments and disputes from third parties in that regard. [461]

---

[458] Antonello Tancredi, "On the Absence of Direct Effect of the WTO Disupte Settlement Body's Decisions in the EU Legal Order", in Enzo Cannizzaro, Paolo Palchetti and Ramses A. Wessel, ed, *International Law as the Law of the European Union*, (Martinus Nijhoff Publishers, Leiden - Boston, 2019): p. 249 et seq.

[459] Argument of the European Court of Justice in the *Kadi* case, regarding the conflict between the European legislation and the obligations deriving from the United Nations Charter.

[460] Stefano Saluzzo, *"*Cross Border Data Flows And International Trade Law. The Relationship Between EU Data Protection Law and the GATS*", Diritto del Commercio Internazionale,* Vol. 4 (2017).

[461] European Commission, Communication From the Commission to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalised World*, COM(2017) 7, January 10, 2017.

CONCLUSION

In the contemporary globalized economy, digital trade and cross-border data flows are strictly connected. International trade negotiations are governed by the flows of data which are at the basis of digital commerce. As a consequence, the global modern society needs rules and regulations always updated to the latest innovations and advances. Thereby, numerous international trade agreements necessarily deal with provisions related to the free flow of data and to privacy protection.

Among different jurisdictions, the European Union holds a prominent position to ensure protection of personal data and promotion of the right to privacy. The global governance of these two rights is strongly influenced by the EU legislative regime, which sometimes has been considered an obstacle to the freedom of trade.

In the framework of the European Union legislation, the people's right to privacy and personal data protection are guaranteed as fundamental human rights, thus assigning them the strongest regulatory value. In particular, the General Data Protection Regulation (GDPR) applies to all international commercial transactions concerning EU individuals' personal data, even if the businesses are not being conducted within the European Union. Consequently, this Regulation affects both European and non-European suppliers of goods and services.[462]

It is clear how the strict connection between international trade, privacy and data protection may collide with national provisions aiming at promoting those fundamental values. For instance, there are some national laws which demand the storage and the processing of personal data in specific local or regional servers, or other national laws which authorize the free flows of data only under the compliance of the service suppliers to specific requirements. The inevitable result is the limitation of digital trade and the disruption of markets' openness.[463]

On the stage of international trade an important role is played by the General Agreement on Trade in Services (GATS), which is the WTO multilateral international agreement applicable to the global trade in services. It deals with data-restrictive

[462] Svetlana Yakovleva, Kristina Irion, "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade", *International Data Privacy Law*, 2020, Vol. 10, No. 3.
[463] *Ibid.*

measures issued by WTO Members providing instruments through which Members may derogate from some obligations without violating the Agreement. This is possible with the General Exceptions set out in Article XIV of the GATS, which give Members a space of freedom in the governance of digital trade to guarantee desired levels of data protection and to ensure the right to privacy to all of their consumers, users and citizens.

However, the scope of this thesis is to find a balance between the openness of international trade and the promotion of the fundamental right to privacy and data protection. The main problems in achieving an effective equilibrium lie in the absence of an international consensus on the protection of personal data and also in the uncertainty of the regulations caused by the constant changes in technologies which require mechanisms and laws for the protection of data always up to date.

The first barrier to trade openness is the different conception that Members have of the notion of privacy and data protection. Each of them interprets those concepts in accordance with the needs and the demands of their societies. For example, in some countries, the right to privacy is considered a fundamental human right and thus, they give a prescriptive geographical approach to data protection different from other countries that look at the privacy notion as a consumer right offering, instead, an accountability-based approach.[464]

However, discordant national legislations make a universally accepted legislative framework on privacy protection more difficult to constitute.

Some international bodies such as the Organization for Economic Co-operation and Development (OECD) have issued guidelines on privacy protection, but they are not mandatory, nor globally recognized neither. This means that these guidelines are not formally relevant under the GATS.

The other obstacle to the achievement of a balance, between trade openness and privacy, regards the constant evolution of the nature of privacy in respect of the changes that the digital world undergoes every day.

Thus, these uncertain and unpredictable circumstances require governments intense efforts to recognize and act thorough their legislations towards the risks which may undermine the right to privacy and personal data protection. To avoid such problems,

[464] Catherine L Mann, "International Internet Governance: Oh What A Tangled Web We Weave" *Georgetown Journal of International Affairs* 2001, Vol. 2, No. 2: 79, 81.

many governments have decided to issue very prescriptive measures such as data-restrictive measures.

As it has been argued throughout the thesis, although these privacy-related data-restrictive measures can breach GATS obligations on non-discrimination, market access, recognition and domestic regulation, Members can justify these measures under the Article XIV of the GATS.

GATS has the strength to provide an actual balance between the economic aspect, facilitating cross-border data flows, and the human rights one, giving Members an opportunity to guarantee the right to privacy and data protection within their territories. Moreover, GATS supports its Members to cooperate among each other and to create and improve interoperability between their respective local legislations[465].

For instance, if two Members have agreed to facilitate the transfer of data between their territories, such an agreement has to be concluded with all the other Members.

Another GATS provision which is beneficial for openness in trade is the one about domestic regulation at Article VI[466]. It can be beneficial to facilitate the recognition of onerous standards or requirements provided by national data protection and privacy laws. An example can be found in case of Members which need digital service suppliers to gain authorizations or permissions for the transfer of data. If Members have committed in their Schedules to open those services to service suppliers or services from abroad, those requirements should be given in a just and fair manner.[467]

The results of this research show that the EU framework for personal data transfers may be found in violation of the EU's international trade commitments, but on the other side, international trade commitments which address completely free transfers of personal data outside the EEA may be found incompatible with the principle enshrined in the EU

[465] General Agreement on Trade in Services, Article VII:1: "For the purposes of the fulfilment, in whole or in part, of its standards or criteria for the authorization, licensing or certification of services suppliers, and subject to the requirements of paragraph 3, a Member may recognize the education or experience obtained, requirements met, or licenses or certifications granted in a particular country. Such recognition, which may be achieved through harmonization or otherwise, may be based upon an agreement or arrangement with the country concerned or may be accorded autonomously."

[466] General Agreement on Trade in Services, Article VI:1: "In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner."

[467] Mishra Neha, "When data flows across borders: Aligning international trade law with internet policy objectives", *University of Melbourne, 2019,* available at https://minerva-access.unimelb.edu.au/handle/11343/233237 (accessed November 10, 2020).

Charter, and in particular with the fundamental rights of privacy and personal data protection.

It is for the protection of these binding fundamental rights, that this situation of non-compliance may result in a scenario where the only solution for the EU is to choose between remaining cohesive to its own "constitutional" framework and fulfilling its trade obligations.

This is the consequence of the incompatibility of the exceptions, and their necessity tests, conceived by the EU and the international agreements to prevent the collision between each other's measures.[468]

After having analyzed, through the thesis, the provisions under the GATS, I would propose an approach to conciliate those provisions with the right to privacy and data protection principles.

First of all, it could be advised a sensible application of GATS provisions on transparency and recognition[469] to encourage trust in the digital trade environment for all the parties involved, such as States, companies, consumers, users, etc. Indeed, if the actors rely more on the WTO system this would be beneficial for the cooperation in the international trade. People do business with whom they can rely and trust and this is true not only in everyday life, but also in economic and commercial affairs. Then, it would be meaningful to involve new subject areas in WTO law, such as obligations or commitments aiming at preventing the issue of data-restrictive measures, favoring cross-border data flows, and at the same time prescribing Members to approve essential frameworks on privacy and data protection, which are common to all the actors.[470]

Outside the system of the GATS, instead, it might be effective to introduce mechanisms to facilitate the dialogue and the international cooperation among international trade actors, to improve the regulatory framework in the context of cross-border data issues, but also to draft a WTO declaration stating the fundamental principles of data flows which cannot be derogated. Furthermore, due to numerous memberships of

---

[468] Svetlana Yakovleva, "Personal Data Transfers in International Trade and EU Law: A Tale of Two 'Necessities'", *Journal of World Investment & Trade* Vol. 21 (2020): 881–919.

[469] General Agreement on Trade in Services, Article VII.

[470] Mishra Neha, "When data flows across borders: Aligning international trade law with internet policy objectives", *University of Melbourne, 2019,* available at https://minerva-access.unimelb.edu.au/handle/11343/233237 (accessed November 10, 2020).

the WTO and, due to the wide consensus, this international organization benefits of, it would be feasible also to support a WTO regulatory assistance in various fora by providing help for the dialogue, encouraging information exchange and cooperation among Members.[471]

In conclusion, notwithstanding the instability and the continuous changes of digital trade and the consequent difficulty in the achievement of an efficient protection of human rights, the WTO, as the most important trade institution, can play a decisive role to provide new and efficient approaches to better balance openness in trade, through the free flow of personal data, with the establishment of a solid and safe legislation to promote the right to privacy and personal data protection.

However, it would be also necessary for the WTO to work alongside with other international and multi-stakeholder institutions in order to build a comprehensive discipline that involves all the most significant dimensions of data regulation and privacy law.

[471] *Ibid.*

BIBLIOGRAPHY

Books

Alastair Mowbray*, Cases, Materials, and Commentary on the European Convention on Human Rights*, 3rd edition, (Oxford: Oxford University Press, 2012)

Alexander Roßnagel, *Europäische Datenschutz-Grundverordnung Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts*, (Seiten, broschiert: Nomos 2017) Anwendungsbereich (2017)

Allan P. Dionisopoulos and Craig Ducat, *The Right to Privacy: Essays and Cases* (St. Paul, Minn, West: Pubhshing Co., 1976)

Antonello Tancredi, "On the Absence of Direct Effect of the WTO Dispute Settlement Body's Decisions in the EU Legal Order", in Enzo Cannizzaro, Paolo Palchetti and Ramses A. Wessel, ed, *International Law as the Law of the European Union*, (Martinus Nijhoff Publishers, Leiden - Boston, 2019)

Christine Chinkin, "Sources", in Daniel Moeckli, Sangeeta Shah, and Sandesh Sivakumaran eds., *International Human Rights Law,* (Oxford: Oxford University Press, 2010)

David Harris, Michael O' Boyle, Ed Bates, and Carla Buckley, *Law of the European Convention on Human Rights*, 2nd edition (Oxford: Oxford University Press, 2009)

Ed Bates, *The Evolution of the European Convention on Human Rights, From Its Inception to the Creation of a Permanent Court of Human Rights,* (Oxford: Oxford University Press, 2010)

European Union Agency for Fundamental Rights, *Handbook on European data protection law,* (Luxemburg: Publication Office of the European Union, 2014)

Gary P. Sampson (ed), "Overview", *The Role of the World Trade Organization in Global Governance*, (Tokyo: United Nations University Press, 2001)

I-Ching Chen, *Government Internet Censorship Measures and International Law,* (Wien, Zweigniederlassung Zurich: LIT VERLAG GmbH & Co. KG, 2018)

James Waldo, Herbert S. Lin, Lynette I. Millett, *Engaging Privacy and Information Technology in a Digital Age,* (Washington, DC: The National Academic Press, 2007)

Jhon H. Jackson, *The World Trade Organization: Constitution and Jurisprudence* (London: Royal Institute of International Affairs, 1998)

John H. Jackson, "Strengthening the International Legal Framework of the GATT-MTN System: Reform Proposals for the New GATT Round." *The New GATT Round of Multilateral Trade Negotiations: Legal and Economic Problems,* edited by E.-U. Petersmann and M. Hilf, 3-23. Studies in Transnational Economic Law, Vol. 5. (Deventer, the Netherlands: Kluwer Law and Taxation Publishers, 1988)

Judith A. Swanson, *The Public and the Private in Aristotle's Political Philosophy*, (Cornell University Press, 1992)

Kalin Walter, Künzli Jorg, *Universeller Menschenrechtsschutz*, 2nd edition, (Basel: Helbing Lichtenhahn, 2008)

Lee A. Bygrave, "Hardwiring Privacy" in Roger Brownsford et al., eds., *The Oxford Handbook of Law, Regulation and Technology,* (Oxford University Press, 2017)

Martix Dixon, *Textbook on International Law,* 7th Edition, (Hampshire: Oxford University Press, 2013)

Mira Burri, "Understanding the Implications of Big Data and Big Data Analytics for Competition Law: An Attempt for a Primer" in *New Developments in Competition Behavioural Law and Economics* eds. Klaus Mathis and Avishalom Tor, (Springer, 2018)

Nadezhda Purtova, *Property Rights in Personal Data: a European Perspective,* (Kluwer Law International 2011)

Nellie Munin, *Legal Guide to GATS,* (Wolters Kluwers, 2010)

Paul Voigt, Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR), A Practical Guide,* (Germany, Hamburg: Springer International Publishing AG 2017)

Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in David Wright and Paul De Hert, *Privacy Impact Assessment,* (Dordrecht Heidelberg London New York: Springer 2012)

Perry Keller, *European and International Media Law: Liberal Democracy, Trade and the New Media* (Oxford University Press, 2011)

Peter Blume, Peter Seipel, Ahti Saarenpää, Dag Wiese Schartum, *Nordic Data Protection*, (Iustus Förlag, Uppsala 2001)

Peter Carey, *Data Protection: A Practical Guide to UK and EU Law,* (United Kingdom: Oxford University Press 2015)

Peter Van den Bosche and Warner Zdouc, *The Law and Policy of the WORLD TRADE ORGANIZATION, Text, Cases and Materials*, 4th ed. (Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press, 2017)

Pietro Pustorino, *Lezioni di tutela internazionale dei diritti umani,* (Bari: Cacucci Editore, 2019)

Rebecca Mackinnon, *Consent of the Networked – The WorldWide Struggle for Internet Freedom,* (New York: Basic Books, 2012)

Rhona K. M. Smith, *International Human Rights Law,* 8th Edition, (Oxford: Oxford University Press, 2018)

Robert Howse and Makau Mutua, "Protecting Human Rights in a Global Economy: Challenges for the World Trade Organization", *International Centre for Human Rights and Democratic Development* (Leiden: Martinus Nijhoff Publishers, 2001)

Robert W. Hahn, *Reviving Regulatory Reform: A Global Perspective*, The AEI Press (Washington, D.C, 2000)

Rolf H. Weber and Mira Burri, *Classification of Services in the Digital Economy*, (Zurich: Schulthess, 2012)

Russell L. Weaver, David F. Partlett, Mark D. Cole, "Protecting Privacy in a Digital Age", in Dieter Dorr, Russell L. Weaver, *The Right to Privacy in the Light of Media Convergence: Perspectives From Three Continent,* (Berlin: De Gruyter, 2012)

Sergio Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, (Padova: CEDAM, 2006)

Stefan Ernst, in Boris P. Paal, Daniel A. Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetx*, Beck'sche Kompakt-Kommentare, (München: Verlag C. H. Beck oHGArt, 2018)

Tatevik Sargsyan, "The Turn To Infrastracture in Privacy Governance" in *The Turn to Infrastructure in Internet Governance,* eds. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, Nanette S. Levinson, (Palgrave Macmillan US, 2015)

Usama Fayyad, Georges G. Grinstein, Andreas Wierse, *Information Visualization in Data Mining and Knowledge Discovery,* (San Francisco: Morgen Kaufman Publisher, 2002)

W. Kuan Hon, *Data Localization Laws and Policy,* (Cheltenham, UK; Northampton, MA, USA: Edward Elgar, 2017)

Won-Mog Choi, *Like Products in International Trade Law,* (Oxford University Press, 2003)

Journals and Articles

Aaditya Mattoo and Joshua P Meltzer, "International Data Flows and Privacy the Conflict and Its Resolution"*, Journal of International Economic Law,* Vol. 21 (2018)

Adamantia Rachovitsa, "Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue", *International Journal of Law and Information Technology* Vol. 24 No. 4 (2016)

Anupam Chander and Uyen P Le, "Data Nationalism" *Emory Law Journal* Vol. 64 No. 3 (2015)

Bashar Malkawi, "Digitalization of Trade in Free Trade Agreements with Reference to the WTO and the USMCA: A Closer Look." *China and WTO Review*, (2019)

Bhaskar Chakravorti, "Why the Rest of the World Can't Free Ride on Europe's GDPR Rules", *Harvard Business Review, https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules* (accessed January 26, 2021).

Blayne Haggart, "The Government's Role in Constructing the Data-driven Economy", *Center for International Governance Innovation,* March 5 2018, available at https://www.cigionline.org/articles/governments-role-constructing-data-driven-economy (accessed November 10, 2020)

Carla L. Reyes, "WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive", *Melbourne Journal of International Law.*

Caroline Dommen, "Safeguarding the Legitimacy of Multilateral Trading System: The Role of Human Rights Law," *in International Trade and Human Rights: Foundations and Conceptual Issues*: eds. Frederick M. Abbott, Christine Greining-Kaufmann, and Thomas Cottier, (Michigan: University of Michigan: The World Trade Forum, Vol. 5, 2006)

Caroline M. Robb, *Can the Poor Influence Policy?* (World Bank: 1998)

Cecilia Malmström, *Speech on TTIP and Trade,* Berlin 2016 available at https://trade.ec.europa.eu/doclib/press/index.cfm?id=1434&title=Speech-Commissioner-Malmstr%C3%B6m-in-Berlin-on-TTIP-and-Trade (accessed August 4, 2020)

Charles Owen Verrill, Jr., Peter S. Jordan, Timothy C. Brightbill, "International Trade", *International Lawyer* Vol. 32 (1998)

Chris Connolly et al, "Privacy self-regulation in crisis? TRUSTee's "deceptive" practices", *UNSW Law Research Paper,* UNSW,(2014)

Christina Gagnier, "Regulating the Man Behind the Curtain", in *Future of the Privacy Forum, Big Data and Privacy: Making Ends Meet,* Stanford Law School the Center of Internet and Society (2013)

Christopher Kuner, "Developing an Adequate Legal Framework for International Data Transfers", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, Sjaak Nouwt eds., *Reinventing Data Protection*? (Springer, 2009)

Christopher Kuner et al, "Internet Balkanization Gathers Pace: Is Privacy the Real Driver?" *International Data Privacy Law* Vol. 5 No. 1 (2015)

Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law", *International Data Privacy Law* Vol.5 No.4 (2015)

Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law" *Bloomberg BNA Privacy and Security Law Report,* (February 2012)

Christopher Kuner, "The European Union and the Search for an International Data Protection Framework" *Groningen Journal of International Law* Vol. 2 No. 2 (2014)

Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", *OECD Digital Economy Papers,* No. 187, OECD Publishing, (2011)

Colum Lynch, "Inside America's Plan to Kill Online Privacy Rights Everywhere", *Foreign Policy: the Cable,* November 20, 2013, https://foreignpolicy.com/2013/11/20/exclusive-inside-americas-plan-to-kill-online-privacy-rights-everywhere/ (accessed March 10, 2020)

Daniel Pruzin, "U.S. Holds E-commerce Talks with WTO Partners, Covering Nature of Digital Products", *International Trade Daily,* Bureau of National Affairs, June 13, (2001)

Dara Hoffman, Elissa How, "Trust in the Balance: Data Protection Laws as Tools for Privacy and Security in the Cloud" 10 *Algorithms* (2017)

Diane A MacDonald and Christine M Streatfield, "Personal Data Privacy and the WTO" *Houston Journal of International Law,* Vol. 36 No. 3 (2014)

eBay Inc and Sidley Austin LLP, *Commerce 3.0 for Development: The Promise of the Global Empowerment Network,* October 2013, https://www.ebaymainstreet.com/sites/default/files/eBay_Commerce-3-for-Development.pdf (accessed August 4, 2020)

Erik van der Marel, Hosuk Lee-Makiyama, Matthias Bauer, "The Costs of Data Localisation: Friendly Fire on Economic Recovery" (ECIPE 2014) https://ecipe.org/publications/dataloc/ (accessed August 17, 2020)

Federica Velli, "The Issue of Data Protection in EU Trade Commitments: Cross-Border Data Transfers in GATS and Bilateral Free Trade Agreements", *European Papers* Vol. 4 No. 3 (European Forum, December 9, 2019)

Fred H. Cate, Christopher Kuner, Dan Jerker B. Svantesson, Orla Lynskey, Christopher Millard, "The Language of Data Privacy Law (and How it Differs from Reality)", *International Data Privacy Law,* Vol.6 No.4 (2016)

Gehan Gunasekara, "Paddling in Unison or Just Paddling? International Trends in Reforming Information Privacy Law*", International Journal of Law and Technology*, Vol. 22, No.2, (2014)

George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, "Privacy and Data Protection by Design – from policy to engineering", *European Union Agency for Network and Information Security,* December 2014, www.enisa.europa.eu (accessed March 21, 2020)

Gilles Muller, "De Facto Discrimination under GATS National Treatment: Has the Genie of Trade Liberalization Been Let Out of the Bottle?", *Legal Issues of Economic Integration*, (2017)

Gráinme de Búrca, "New governance and experimentalism: An introduction. Symposium Issue on New Governance and the Transformation of Law", *Wisconsin Law Review*, (2010)

James Manyika et al, "Digital Globalization: The New Era of Global Flows" (McKinsey Global Institute, March 2016):1 http://www.mckinsey.com/business-functions/digital-mckinsey/our- insights/digital-globalization-the-new-era-of-global-flows (accessed July 19, 2020)

James Waldo, Herbert S. Lin, and Lynette I. Millett eds., "Thinking about privacy: Chapter 1 of Engaging Privacy and Information Technology in Digital Age", Journal of Privacy and Confidentiality, Vol. 2, No.1 (2010)

Jennifer Daskal, "The Un-Territoriality of Data", Vol. 125 No. 2, *Yale Law Journal* (2015)

Joshua P. Meltzer, "A New Digital Trade Agenda". *E15Initiative*. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, 2015. www.e15initiative.org/. (Accessed June 11, 2020)

Joshua P Meltzer, "The Internet, Cross-Border Data Flows and International Trade", *Asia & the Pacific Policy Studies* Vol. 2 (2014)

Jessica Nicholson and Ryan Noonan, "Digital Economy and Cross-Border Trade: The Value of Digitally- Deliverable Services", *US Department of Commerce Economics and Statistics Administration*, ESA Issue Brief no 1-14, (2014)

Katherine Connolly, "Finding Space for Regulatory Autonomy in GATS Article XVII after *EC – Seals:* Public Services and the "Likeness" of Public and Private Service Providers", *Legal Issues of Economic Integration* Vol. 42 No.1 (2015)

Konstantinos Komaitis, "The "Wicked Problem" of Data Localization", *Journal of Cyber Policy* Vol. 3, No. 2 (2017)

Kristi L. Bergemann, "A Digital Free Trade Zone and Necessarily-Regulated Self-Governance for Electronic Commerce: The World Trade Organization, International Law, and Classical Liberalism in Cyberspace", *Marshall Journal of Computer and Information Law* Vol. 20, (2002)

Kristina Irion, Svetlana Yakovleva and Marija Bartl, "Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements", *independent study commissioned by BEUC et al*., (Amsterdam: Institute for Information Law (IViR), July 13, 2016)

Martina Ferracane, "Data Flows & National Security: A conceptual framework to assess restrictions on data flows under GATS security exception", *GigaNet: Global Internet Governance Academic Network, Annual Symposium,* (2018)

Martina Ferracane, Hosuk Lee Makiyama and Erik van der Marel "Digital Trade Restrictiveness Index", *European Centre For International Political Economy, Digital Trade Estimates.* http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2018/09/DTRI-final.pdf (accessed August 10, 2020)

MCEJ Bronckers, "More Power to the WTO?", *Journal of International Economic Law,* (2001)

Merlin Gömann, "The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement", *Common Market Law Review*, (2017)

Mira Burri and Rahel Schär, "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", *Journal of Information Policy,* Vol. 6 (2016)

Mishra Neha, "When data flows across borders: Aligning international trade law with internet policy objectives", *University of Melbourne, 2019,* available at https://minerva-access.unimelb.edu.au/handle/11343/233237 (accessed November 10, 2020)

Nigel Cory, "Cross-Border Data Flows: Where are the Barriers and What Do They Cost?" (May 2017): 3 – 4. https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost (accessed August 15, 2020)

Nivedita Sen, "Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?" *Journal of International Economic Law,* Oxford University Press, Vol. 21 No. 2, (2018)

Noam Tirosh, "Reconsidering the "Right to be Forgotten" – memory rights and the right to memory in the new media era", *Media, Culture and Society,* Vol 39, no 5, (2017)

Oliver Diggelmann, Maria Nicole Cleis, "How the Right to Privacy Became a Human Right", Human Rights Law Review, (2014)

Panagiotis Delimatsis, "International Trade in Services and Domestic Regulations, Necessity, Transparency and Regulatory Diversity", *International Economic Law*, (2007)

Panagiotis Delimatsis, Martin Molinuevo, “Article XVI GATS: Market Access”, *Max Planck Commentaries on World Trade Law, WTO- Trade in Services,* in Rüdiger Wolfrum, Peter-Tobias Stoll, Clemens Feinäugle, eds., Vol 6 (Leiden/Boston: Martinus Nijhoff Publishers, 2008). Available at SSRN: https://ssrn.com/abstract=1280219. (accessed September 3, 2020)

Paul de Hert and Michal Czerniawski, “Expanding the European Data Protection Scope beyond Territory: Article 3 of the General Data Protection Regulation in its Wider Context”, *International Data Privacy Law* Vol. 6 Issue 3, (2016)

Peter Blume, “The data Subject”, *European Data Protection Law Review,* (2015)

Peter P. Swire, “Elephants and Mice Revisited: Law and Choice of Law on the Internet”, *University of Pennsylvania Law Review* Vol. 153, (2005)

Peter Traung, “The Proposed New EU General Data Protection Regulation—Further Opportunities”, *Computer Law Review International*, Vol. 2, (2012)

Philippa Dee, “A Compendium of Barriers to Services Trade” (World Bank, 2005)

Rachel Harris and Gillian Moon, “GATT Article XX and Human Rights: What Do We Know form the First 20 Years”, *Melbourne Journal of International Law*, (2015)

Robert C. Post, "Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere," *Duke Law Journal* Vol 67, no. 5 (2018)

Rolf H Weber, “Regulatory Autonomy and Privacy Standards under the GATS” *Asian Journal of WTO and International Health Law & Policy* Vol. 7 (2012)

Rolf H. Weber, "Transborder data transfer: concepts, regulatory approaches and new legislative initiatives", *International Data Privacy Law*, Vol. 3, Issue 2, (2013)

Ruosi Zhang, "Covered or Not Covered: That Is the Question - Services Classification and Its Implications for Specific Commitments under the GATS", *WTO Staff Working Papers from World Trade Organization (WTO), Economic Research and Statistics Division,* No. ERSD-2015-11, f (2015)

Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review,* Vol. 4, No. 5 (1890)

Sergey Brin and Lawrance Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine", *Seventh International World-Wide Web Conference*, *WWW 1998*, (1998)

Shin-yi Peng and Han-wei Liu, "The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?" *Journal of World Trade* Vol.51 No. 2 (2017)

Stephan Haggard and Steven B. Webb, eds., *The World Bank Participation Sourcebook*, (World Bank: 1996)

Stefano Rodotà, "Riservatezza", *Treccani*, Enciclopedia Italiana – VII Appendice (2007), http://www.treccani.it/enciclopedia/riservatezza_res-9e2b210a-9bc7-11e2-9d1b-00271042e8d9_(Enciclopedia-Italiana)/. (accessed February 11, 2020)

Stefano Saluzzo, "Cross Border Data Flows and International Trade Law. The Relationship Between EU Data Protection Law and the GATS", *Diritto del Commercio Internazionale,* Vol. 4. (2017)

Stephen M. Schwebel, "The Effect of Resolutions of the U.N. General Assembly on Customary International Law", Proceedings of the Annual Meeting, *American Society of International Law,* Vol. 73, (April 26-28, 1979)

Stewart A. Baker, Peter Lichtenbaum, Maury D. Shenk, Matthew S. Yeo, "E-Products and the WTO*" International Lawyer* Vol. 35, (2001)

Susan A. Aaronson, Patrick Leblond, "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO", *Journal of International Economic Law* Vol. 21 No. 2, Oxford University Press (2018)

Svetlana Yakovleva and Kristina Irion, "The Best of Both Worlds – Free Trade in Services and EU Law on Privacy and Data Protection", *European Data Protection Law Review* (2016)

Svetlana Yakovleva, "Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"?", *World Trade Review,* Vol. 17 No. 3 (2018)

Tania Voon, "Exploring the Meaning of Trade Restrictiveness in the WTO", *World Trade Review* Vol. 14 No. 3 (2015)

Taunya L. McLarty "Liberalized Telecommunications Trade in the WTO: Implications for Universal Service Policy", *Federal Communications Law Journal*, Vol. 51 (1998)

Thomas Cottier, "Trade and Human Rights – A Relationship to Discover"*, Journal of International Economic Law*, Vol.5, (2006)

Tim Maurer, Robert Morgus, Isabel Skierka and Mirko Hohmann, "Technological Sovereignty: Missing the Point?" in *Architectures in Cyberspace* eds. M. Maybaum, A. - M. Osula, L.Lindstöm, (NATO CCD COE Publications, 2015)

Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Natalia Torres, "Global Survey on Internet Privacy and Freedom of Expression"*, United Nations Educational, Scientific and Cultural Organization* (2012)

Treccani, "GATS (General Agreement on Trade in Services)", *Dizionario di Economia e Finanza (2012),* available at https://www.treccani.it/enciclopedia/gats_%28Dizionario-di-Economia-e-Finanza%29/ (accessed March 17, 2020)

Usama Fayyad, "The Digital Physics of Data Mining"*, Communications of ACM*, Vol. 44, Issue 3 (2001)

Usman Ahmed and Anupam Chander, "Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows" *Think Piece*, E15 Expert Group on the Digital Economy, (2015)

W Kuan Hon, Christopher Millard, Jatinder Singh, Ian Walden, Jon Crowcroft, "Policy, Legal and Regulatory Implications of a Europe-only Cloud", *International Journal of Law and Information Technology,* Vol. 24, No. 3 (2016)

Wafa Tim, "Global Internet Privacy Rights – A Pragmatic Approach*", University of San Francisco Intellectual Property Law Bulletin*, Vol. 13, (2009)

William J. Drake and Kalypso Nicholaidis, "Global Electronic Commerce and the General Agreement on Trade in Services: The "Millennium Round" and Beyond" in *GATS 2000: New Directions in Services Trade Liberalization,* eds. Pierre Sauve and Robert M Stern, *Liberalization* The Brookings Institution, (2000)

William J. Drake, Vinton G. Cerf, Wolfgang Kleinwächter, "Internet Fragmentation: An Overview" *Future of the Internet Initiative White Paper*, World Economic Forum, (2016)

Online Documents and Reports

Asia-Pacific Economic Cooperation, https://www.apec.org/About-Us/About-APEC.

Commission Implementing Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided By the EU-U.S. Privacy Shield, *Decision C(2016) 4176 final*, July 12, 2016, ('EU−US Privacy Shield')

Communication from Japan, *Joint Statement on Electronic Commerce Initiative*, WTO Doc INF/ECOM/4 March 25, 2019

Communication from the African Group, "Work Programme on Electronic Commerce", *Report of Panel Discussion on 'Digital Industrial Policy and Development'*, WTO Doc JOB/GC/133 July 21, 2017.

Communication from the US, *Joint Statement on Electronic Commerce*, WTO Doc INF/ECOM/23 April 26, 2019

Congressional Research Service, *Digital Trade and US Trade Policy*, 21 May 2019, https://fas.org/sgp/crs/misc/R44565.pdf (accessed June 17, 2020)

Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 1 (The Hague: Martinus Nijhoff, 1975)

Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 3 (The Hague: Martinus Nijhoff, 1976)

Council of Europe, "Collected Edition of the 'Travaux Preparatoires' of the European Convention on Human Rights", Vol. 4 (The Hague: Martinus Nijhoff, 1977)

Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *European Treaty Series – No. 108,* Strasbourg, 28.l.1981

Council of Europe, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Consultative Committee of the convention for the protection of individuals with regard to automatic processing of personal data, (Strasbourg: January 23, 2017).

Council of Europe Portal, *Convention 108 and Protocols,* https://www.coe.int/en/web/data-protection/convention108-and-protocol (accessed March 12, 2020)

Council of Europe Portal, *Council of Europe in brief,* https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (accessed January 5, 2021).

Discussion Draft, "Benefits of the APEC Cross-Border Privacy Rules, Protecting Information. Driving Growth. Enabling Innovation*",* https://www.crowell.com/files/20181001-Benefits-of-CBPR-System%20Guide_Oct%202018_final.pdf (accessed March 12, 2020)

Drafting Commission Report 21, Annex A, (Secretariat Outline)

Drafting Commission Report 21, Annex D, ('Cassin Draft')

Drafting Commission Report 21, Annex F, ('Revised Cassin Draft')

Drafting Committee on an International Bill of Human Rights, Report on its 1st Session, July 1, 1947, *E/CN.4/21* ('Drafting Commission Report 21') at Annex A

ECIPE, "Digital Trade Estimates Database" https://ecipe.org/dte/database/?country=&chapter=829&subchapter=830 (accessed September 20, 2020)

Equality and Human Rights Commission, *What is the Charter of Fundamental Rights of the European Union?* https://www.equalityhumanrights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union

European Commission, "Adequacy Decisions, how the EU determines if a non-EU country has an adequate level of data protection", available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed August 3, 2020)

European Communities and their Member States - *Schedule of Specific Commitments*, GATS/SC/31, April 15, 1994 available at https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=31391,10335,2244,15832,33570,37471,26509&CurrentCatalogueIdIndex=6&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True (accessed September 14, 2020)

European Commission, Communication From the Commission to the European Parliament and the Council, *Exchanging and Protecting Personal Data in a Globalised World*, COM(2017) 7, January 10, 2017

European Commission, Directive 95/46/EC, https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en

European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", *COM(2012) 11 final*, January 25, 2012

European Commission, Services and investment in EU trade deals: Using "positive" and "negative" lists, April 2016,

<http://trade.ec.europa.eu/doclib/docs/2016/april/tradoc_154427.pdf (accessed June 17, 2020)

European Commission, "WEU-US Privacy Shield: Second Review Shows Improvements but a Permanent Ombudsperson Should be Nominated by 28 February 2019" (Press Release, December 19, 2018) available at <http://europa.eu/rapid/press-release_IP-18-6818_en.htm>. (accessed August 3, 2020)

European Court of Human Rights, *European Convention on Human Rights,* *https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c* (accessed January 5, 2021)

European Data Protection Supervisor, "Data Protection", available at <https://edps.europa.eu/data-protection_en> (accessed June 4, 2020)

European Data Protection Supervisor, *The History of the General Data Protection Regulation,* *https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=It%20replaces%20the1995%20Data%20Protection,their%20countries%20by%20May%202018.* (accessed January 5, 2021)

European Union, "What is GDPR, the EU's new data protection law?" *GDPR.EU,* https://gdpr.eu/what-is-gdpr/, (accessed March 4, 2020)

GATT BISD, Volume IV

GATT Doc. No. MTN.GNG/NG14/W/42, *Communication from the European Community,* dated 9 July 1990

GATT Doc. MTN.TNC/W/FA, *Draft Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations*, 20 December 1991

GATT MIN.DEC, *Ministerial Declaration on the Uruguay Round,* dated 20 September 1986, Part I, Section E, "Functioning of the GATT System"

Global Network Initiative, "GNI Principles on Freedom of Expression and Privacy" (2008), http://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf. (accessed March 5, 2020)

ICC Commission on Trade and Investment Policy and ICC Commission on the Digital Economy, "Trade in the Digital Economy—A Primer on Global Data Flows for Policymakers" *International Chamber of Commerce (ICC)*, 2016, Policy Paper 103/330, 373/560 1 https://iccwbo.org/publication/trade-in-the-digital-economy/ (accessed August 12, 2020)

Internet Code of Practice (Singapore), 1 November 1997, art 4; US Department of Homeland Security, "DHS Statement on the Issuance of Binding Operational Directive 17- 01" *Homeland Security,* Press Release, September 13, 2017, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01 (accessed July 22, 2020)

Intersoft Consulting, "General Data Protection Regulation, GDPR", available at https://gdpr-info.eu (accessed March 1, 2020)

Organization for Economic Co-operation and Development, "Better Policies for Better Lives", http://www.oecd.org/about/ (accessed March 7, 2020)

Organization for Economic Co-Operation and Development, *OECD Privacy Guidelines*, https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm (accessed January 05, 2020).

OHCHR, The International Bill of Rights Fact Sheet 2, Rev 1, available at https://www.ohchr.org/documents/publications/factsheet2rev.1en.pdf (accessed June 12, 2020)

The Global Network Initiative, "2014 Annual Report Protecting and Advancing Freedom of Expression and Privacy in Information and Communication Technologies", *GNI* (2014)

The World Commission on Environment and Development, "Our Common Future", *Oxford University Press*, (1987).

UN Economic and Social Council, *Statement of the UN Committee on Economic, Social and Cultural Rights to the Third Ministerial Conference of the World Trade Organization (Seattle, 30 November to 3 December 1999),* UN Doc. E/C.12/1999/9, Geneva: 26 November 1999

UN General Assembly, "Guidelines for the Regulation of Computerized Personal Data Files", *A/RES/45/95,* December 34, 1990

UN Human Rights Committee General Comment 16, 23.03.1988, *UN Doc a/43/40*

UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development,* New York and Geneva (2016).

UNCTAD, Data Protection and Privacy Legislation Worldwide, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed May 1st, 2020)

UNCTAD, "Summary of Adoption of E-Commerce Legislation Worldwide" https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx (accessed March 10, 2020)

United Nations, General Assembly, "The right to privacy in the digital age", Seventy-first session, Third Committee, November 16, 2016

United Nations Human Rights, Office of the High Commissioner, "Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression", *Human Rights Council*, *U.N. Doc. A/HRC/23/40*, April 17, 2013

United Nations Human Rights, Office of the High Commissioner, "The Right to Privacy in the Digital Age", *G.A. Res. 68/167, U.N. Doc. A/RES/68/167*, December 18, 2014

United Nations, "Reflection on Data Privacy", *Office of Information and Communications Technology*, https://unite.un.org/news/reflections-data-privacy (accessed March 7, 2020)

United Nations, *Sustainable Development Goals.* https://www.un.org/sustainabledevelopment/sustainable-development-goals/ (accessed May 12, 2020)

United Nations, "The Right to Privacy in the Digital Age", *United Nations Human Rights Office of the High Commissioner,* https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx#:~:text=The%20General%20Assembly%20affirmed%20that,to%20privacy%20in%20digital%20communication.&text=It%20further%20states%20that%20%E2%80%9CEveryone,against%20such%20interference%20or%20attacks.%E2%80%9D (accessed March 7, 2020)

US - China Business Council, "Optimizing Connectivity: Updated Recommendations to Improve China's Information Technology Environment" (February 2018) https://www.uschina.org/sites/default/files/uscbc_ict_recommendations_en.pdf (accessed September 11, 2020)

World Trade Organization, “20 Years of the Information Technology Agreement”, https://www.wto.org/english/res_e/booksp_e/ita20years_2017_chap2_e.pdf (accessed May 30, 2020)

World Trade Organization Annual Report 2016

World Trade Organization Appellate Body Report, *Argentina – Financial Services,* 2016

World Trade Organization Appellate Body Report, *Brazil – Retreaded Tyres,* 2007

World Trade Organization Appellate Body Report, *Canada – Autos,* 2000

World Trade Organization Appellate Body Report, *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, 2009

World Trade Organization Appellate Body Report, *EC-Bananas III,* 1997

World Trade Organization Appellate Body Report, *EC – Seal Products,* 2013

World Trade Organization, Appellate Body Report, *Korea - Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, 2000

World Trade Organization Appellate Body Report, *Mexico – Taxes on Soft Drinks,* 2006

World Trade Organization Appellate Body Report, *Thailand – Cigarettes (Philippines),* 2011

World Trade Organization Appellate Body Report, *US –Gambling,* 2005

World Trade Organization Appellate Body Report, *US — Gasoline,* 1996

World Trade Organization, Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, 2005

World Trade Organization Appellate Body Report, *US – Shrimp (Thailand),* 2008

World Trade Organization Dispute Settlement Body, Appellate Body Report, *Antigua and Barbuda v. United States, US-Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, 2005

World Trade Organization, *Doha Development Agenda: July 2008 Package: How the meeting was organized.* https://www.wto.org/english/tratop_e/dda_e/meet08_org_e.htm (accessed March 14, 2020)

World Trade Organization, *GATS Basic Purpose and Concepts*, https://www.wto.org/english/tratop_e/serv_e/cbt_course_e/c1s7p1_e.htm (accessed January 19, 2021).

World Trade Organization, Ministerial Conference, *Doha Ministerial Declaration,* 9-14 November 2001, WT/MIN(01)/DEC/1, Doha, 20 November 2001

World Trade Organization, *Overview: the TRIPS Agreement*, https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm

World Trade Organization, *General Agreement on Tariffs and Trade 1994,* https://www.wto.org/english/docs_e/legal_e/06-gatt_e.htm

World Trade Organization Panel Report, *Australia — Tobacco Plain Packaging,* 2018

World Trade Organization Panel Report, *China —Auto Parts,* 2008

World Trade Organization Panel Report, *Colombia – Ports of Entry,* 2009

World Trade Organization Panel Report, *EC – Bananas III,* 1997

World Trade Organization Panel Report, *Ecuador, Guatemala Honduras, Mexico and United States v. European Communities,* 1997

World Trade Organization Panel Report, *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, 2009

World Trade Organization Panel Report, *China – Rare Earths,* 2014

World Trade Organization Panel Report, *US – Gambling*, 2004

World Trade Organization, *The General Agreement on Trade in Services (GATS): objectives, coverage and disciplines*, https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm

World Trade Organization, "The WTO", available at https://www.wto.org/english/thewto_e/thewto_e.htm (accessed March 17, 2020)

World Trade Organization, "Trade Rules for the Digital Economy: Charting New Waters at the WTO", *World Trade Review* Vol. 18 (2019), WTO, *Understanding the WTO: Settling Disputes: a unique contribution, https://www.wto.org/english/thewto_e/whatis_e/tif_e/disp1_e.htm*

World Trade Organization, *World Trade Report,* 2012

Miscellaneous

Argument of the European Court of Justice in the *Kadi* case, regarding the conflict between the European legislation and the obligations deriving from the United Nations Charter

Beschluss des Rates der IT-Beauftragten der Ressorts (Germany), Beschluss Nr 2015/5, July 29, 2015; Decree on the Management, Provision and Use of Internet Services and Online Information (Vietnam), Decree No 72/2013/ND-CP, art 4.4, art 5, July 15, 2013; Undang-Undang Tentang Pelayanan Publik (Indonesia), Law No 25/2009, July 18, 2009

Economics and Statistics Administration and the National Telecommunications and Information Administration, *Measuring the Value of Cross-Border Data Flows*, US Department of Commerce, September 2016

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013

UNESCO, "Keynotes to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy and Ethics on a Global Internet"*, United Nation Education, Scientific and Cultural Organization*, Draft Study, Connecting the Dots conference, Paris, UNESCO Headquarters March 3-4, 2015

United States International Trade Commission, *Digital Trade in the US and Global Economies*, Part 2, Publication No 4485, August 2014

United States International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*, Publication number 4716, Investigation Number 332-561, August 2017

World Trade Organization, *Ministerial Declaration on Trade in Information Technology Products*, December 13, 1996

World Trade Organization, *Services Sector Classification List*, MTN.GNS/W/120, July 10, 1991

WTO Secretariat, *Development Implications of Electronic Commerce*, WT/COMTD/w/51, November 23, 1998

Legislation

Asia-Pacific Economic Cooperation Privacy Framework, 2005

Asia-Pacific Economic Privacy Framework, 2015

Agreement on the European Economic Area, 1993

Charter of Fundamental Rights of the European Union, 2000

Charter of The United Nations, 1945

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS. No 108, 1985

Convention on the Protection of Human Rights and Fundamental Freedoms, 1953

Cybersecurity Law (People's Republic of China), 2017

Data Protective Directive, 95/46/EC, 1995

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

Dispute Settlement Understanding on rules and procedures governing the settlement of disputes, 1995

European Charter of Fundamental Rights.

European Convention for the Protection of Human Rights and Fundamental Freedoms, 1953

General Agreement on Tariffs and Trade, 1947

General Agreement on Trade in Services, 1995

Regulation (EU) 2016/679, General Data Protection Regulation

International Covenant on Civil and Political Rights, 1976

International Covenant on Economic, Social and Cultural Rights, 1976

Law on Network Information Security (Vietnam), No. 86/2015/QH13, 2016

Marrakesh Agreement Establishing the World Trade Organization, 1994

OECD Privacy Framework

Universal Declaration of Human Rights, 1948

Case Law

Court of Justice of the European Union, Case C-136/17, *GC, AF, BH, ED v Commission nationale de l'informatique et des libertés (CNIL)*

Court of Justice of the European Union, *Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others*, and C-520/18, Ordre des barreaux francophones et germanophone and Others, Luxembourg, 6 October 2020.

Court of Justice of the Euopean Union, *Opinion 1/15 (n 1)*

European Court of Human Rights, "Ben Faiza v. France"*, ECHR 050,* 2018

European Court of Human Rights, *Gaughran v. the United Kingdom,* February 13, 2020.

European Court of Human Rights, "Leander v. Sweden", *Application No. 9248/81*, 1987

European Court of Human Rights, "Murray v. The United Kingdom"*, Application No. 14310/88,* 1994

European Court of Human Rights, *Personal data protection, S. and Marper v. the United Kingdom*

European Court of Human Rights, *Personal data protection, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*

European Court of Human Rights, “Von Hannover v. Germany”, *Application No. 59320/00*, 2004

European Court of Justice, “Asociacion Nacional de Establecimientos Financiarios de Crédito and Federacion de Comercio Electronico y Marketing Directo v. Administracion del Estado”, *Joined cases C-468/10 and C-469/10*, 2011

European Court of Justice, “Google Spain, C-131/12”, ruling of May 13, 2014

European Court of Justice, “Heinz Huber v. Bundesrepublik Deutschland*”, C-542/06,* 2008

United States Court of Appeals, Second Circuit, *Dolly M. E. Filartiga and Joel Filartiga, Plaintiffs-Appellants, v. Americo Norberto Pena-Irala, Defendant-Appellee,* No. 191, Docket 79-6090, 1980