Lebanese University

Faculty of Law and Political and Administrative Sciences

The Deanship

ADR IN THE DIGITAL AGE: BETWEEN DATA PROTECTION, INFORMATION TECHNOLOGY and CYBERSECURITY

A Dissertation Fulfilled Under the Partial Requirements for Obtaining a Master's Degree in Business Law

Prepared by

Ibrahim Saad Eddine Saad El-Masri

Members of the Jury

Dr. Marie-Line Karam	**Supervising Professor**	**President**
Dr. Georges El-Ahmar	**Assistant Professor**	**Member**
Dr. Leila Nicolas	**Assistant Professor**	**Member**

2021

The Lebanese University is not responsible for the views and opinions expressed in this dissertation as it only expresses those of the author.

Dedication

For my Father, death cannot kill what never dies. Thank you for watching over me. This is for you. May your beautiful soul rest in peace.

For my Mother, I am who I am because of you. Everything I achieve I owe to you.

For my Brother and Sister, you've set the bar high in every conceivable way and I'm just trying to reach it.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my advisor Dr. Marie-Line Karam. Thank you for your invaluable guidance, expertise, and knowledge. You've dedicated so much time and effort by venturing with me through the intricacies of this topic and made sure that we reached our desired outcome. To have someone of your stature as my advisor made everything easier. It has been a pleasure.

A huge debt of gratitude is also owed to Dr. Georges El-Ahmar and Dr. Leila Nicolas. Thank you for taking on the role of being jury members and devoting your valuable time and knowledge to reading, constructively criticizing, and enhancing the contents of this thesis.

Finally, I would like to sincerely acknowledge my family and friends. This is their work as much as it is mine. Thank you for your unwavering support, sacrifices, guidance, insightful suggestions, and patience.

List of Abbreviations and Acronyms

AAA- American Arbitration Association

ABA- American Bar Association

AI- Artificial Intelligence

ADR- Alternative Dispute Resolution

BCR- Binding Corporate Rules

CIArb- Chartered Institute of Arbitrators

CJEU- Court of Justice of the European Union

CNIL- Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)

CPR- International Institute for Conflict Prevention and Resolution

C2P- Controller to Processor

DDoS- Distributed Denial of Service

DoS- Denial of Service

DPA- Data Protection Authority

DPC- Data Protection Commission

DPO- Data Protection Officer

DPD- Data Protection Directive

ECHR- European Convention on the Protection of Human Rights and Fundamental Freedoms

EC- European Commission

ECJ- European Court of Justice

EDPR- European Data Protection Board

FCC- Federal Communications Commission

FTC- Federal Trade Commission

GDPR- General Data Protection Regulation

ICC- International Chamber of Commerce

ICCA- International Commercial Court of Arbitration

ICDR- International Center for Dispute Resolution

ICSID- International Center for Settlement of Investment Disputes

ICT- Information and Communication Technology

IT- Information Technology

LCIA- London Court of International Arbitration

LLC- Limited Liability Company

NDA- Non-Disclosure Agreement

NSA- National Surveillance Agency

ODR- Online Dispute Resolution

OECD- Organization for Economic Cooperation and Development

PCA- Permanent Court of Arbitration PRISM- Planning Tool for Resource Integration, Synchronization, and Management

Rec- Recital

TFEU- Treaty on the Functioning of the European Union

SCC- Standard Contract Clauses

SEC- Securities and Exchange Commission

SME- Small-Medium Establishment

UNCITRAL- United Nations Commission on International Trade Law

WP29- Working Party 29

WIPO- World Intellectual Property Organization

Abstract

Introduction

"Every country, company, and individual is now being enlisted in the technological revolution as either a subject or an object[1]." - Henry Kissinger

For most of human history, never before was there a more impactful proliferation than the one witnessed in the 21st century through the surge of digitalization. Customarily, new ideas, technologies, and innovations were built on previous concepts and took multiple decades to achieve their culmination, which was defined by the ripples they caused across several other physical plains. Although the same could be said about technology and digitalization, in the sense that they were based on certain precedents which fulfilled the concept of moving from one to many rather than zero to one. However, the unparalleled rate of acceleration in this field propelled it to reach a faster worldwide impact in comparison to other ingenuities over time. Moreover, their ripples forced the creation of another plain outside the physical world; a virtual concept coined as "cyberspace"[2]. Thus, humanity witnessed the creation of a new frontier undefined and undetermined by the concept of precedent dependency. Hence, a technological revolution of unperceived consequences on both the physical and the virtual world caught international communities, countries, policymakers, companies, and individuals off-guard. Therefore, global digitalization reshuffled the power statuses, economic capabilities, local and foreign policies, and international relations of countries, and affected the individual rights of people.

One of the most important consequences that the digital era has had on countries and individuals specifically was the alteration in the perception of privacy. Privacy went from a term used by philosophers such as Aristotle to differentiate between "inner" and "outer", private and

[1] Henry Kissinger, World Order, published by the Penguin Group, USA, New York, 2014, pages 343, 344

[2] The word "Cyber" was introduced by Norbert Wiener in his book "Cybernetics: Control and Communication in the Animal and the Machine", 1948. It was a reference to human beings as nodes in communication rather than machines. However, the term cyberspace in relative terms was used by science fiction writer Ford Gibson, in his novel "Neuromancer" in 1984. It described a cybernetic space that is not identical with the three-dimensional physical space; it's a place that barely simulates the real one.

public, solitude and society[3], to a fundamental human right in need of protection from physical and later digital trespass. In regards to the concept of privacy, history can be arranged into four different periods based on impactful events that diversified and remodeled this notion. The first period extended from the 14th century until the 18th century, where privacy was affiliated with family life, personal correspondence, and the privacy of houses. Physical actions such as trespassing, eavesdropping, or opening sealed letters and reading them were breaches of privacy that were penalized by courts. One of the earliest cases brought to courts was about eavesdropping and home intrusions. This fact could be attributed to the Justices of Peace Act in England in 1361, which provided for the arrest of trespassers[4]. Also, in relation to trespass and seizure of physical property, British Lord Camden in *Entick v. Carrington* (1765) annulled a warrant to enter a house and seize papers. He deemed that such acts were illegal and unjustifiable under the British laws, however, if they were, such actions would completely ruin all comforts of society, since papers are considered as the most valuable property owned by man[5]. In 1791, the Fourth Amendment was laid down as part of the U.S. Constitution, it forbids unreasonable searches and seizures of individuals and properties from official and unofficial intrusions[6]. The second period extended from the mid-19th century to the 1970s. It can be attributed to the widespread and involvement of the press in peoples' daily lives which sparked a movement towards another change of perception in regards to privacy. Newspapers and the press with their constant search for information in which they would resort to any length to find out certain truths have resulted in the exploitation of individuals' privacy on a commercial level. In 1873, complaints surrounding the interviewing techniques of journalists were voiced[7]. In July 1890 E.L. Godkin wrote that the primary enemy of privacy in modern times is the inquisitiveness demonstrated by people concerning the affairs of other people[8]. Following that, the integration of

[3] Stanford Encyclopedia of Philosophy, Privacy, published May 14, 2002; revised January 18, 2018, found at https://plato.stanford.edu/entries/privacy/ visitation date 12/2/2020

[4] Justices of the Peace Act 1361, Chapter 1,34 Edw 3

[5] Entick v. Carrington (1765) 19 St. Tr. 1030, found at https://learninglink.oup.com/static/5c0e79ef50eddf00160f35ad/casebook_19.htm visitation date 12/2/2020

[6] See https://constitution.congress.gov/constitution/amendment-4/ visitation date 12/2/2020

[7] Jan Holvast, History of Privacy, Part of a book by: V. Matyáš et al. (Eds.): The Future of Identity, IFIP AICT 298, published by Springer Nature, Switzerland, 2009, pp. 13-42, page used 19 found at https://link.springer.com/content/pdf/10.1007%2F978-3-642-03315-5_2.pdf visitation date 15/5/2020

[8] Robert Mathews, Interrogation "privacy" in a world brimming with high political entanglements, surveillance, interdependence & interconnections, Article in "Health and Technology", Issue 7, 2017, pp. 265-324, page used 286

instantaneous photography and the increase in press capabilities led to the revolutionary and groundbreaking article published in 1890 by Louis Brandeis and Samuel Warren in the Harvard Law Review titled "The Right to Privacy"[9]. It recognized that the right to privacy is more than just for physical protection from interference with life and property. Accordingly, it should be broadly defined in conjunction with and outside the scope of progression that the "right to life" has had throughout time, which previously only dealt with cases of assault and battery, and evolved to what was known as the 'right to enjoy life" and the "right to be let alone". Thus, the new "Right to Privacy" should offer and secure the utilization of civil privileges against the vilification and obtrusion on a person's thoughts, emotions, sensations, and property whether tangible or intangible[10]. The influence of this article and other writings was felt in 1902 in *Roberson v. Rochester Folding Box Co.*[11], in which a local milling company decided to use a photo of a girl called Abigail Rochester to promote their product. Accordingly, her photo was displayed in several stores, warehouses, and saloons. Consequently, Abigail claimed that she had a 'right of privacy' and brought forward a suit of $15,000. Her suit was denied by the New York Court since her claim had no legal backing in the common law and no legally acknowledged rights were infringed. However, the decision was taken by a simple majority of 4-3, and the mere consideration of such a right was a step forward. The spark ignited by the previous case was realized three years later in *Pavesich v. New England Life Insurance Co*[12]. In short, the picture of a man named Paolo Pavesich was also used to promote the image of a life insurance company without his consent. The advertisement compared his image, being that of a healthy man who bought insurance, to an image of another sickly man without insurance with a quote underneath it. Accordingly, he filed a claim against the company and asked for $25,000 worth of damages. His claim was unanimously accepted based on the invasion of his privacy right. This case became a strong precedent for privacy violation based on the unauthorized use of an individual's picture. The aforementioned period can be regarded as the period of raising awareness about

[9] Louis Brandeis, Samuel Warren, "The Right to Privacy", Article, published in Harvard Law Review, Volume 4, Issue No. 5, December 15, 1890, pp.193-220, page used 193 found at https://www.jstor.org/stable/i256795 visitation date 25/3/2020.
[10] Ibid, pp. 194-196
[11] Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902), case details found at https://casetext.com/case/roberson-v-rochester-folding-box-co-1/?PHONE_NUMBER_GROUP=P
[12] Pavesich v. New England Life Ins. Co., 122 Ga. 190 (Ga. 1905), case details found at https://casetext.com/case/pavesich-v-new-england-life-ins-co

privacy and its status as a human right outside the norms of just physical intrusion. It was supplemented by many articles and books which paved the way for the third phase of securing privacy. The third period- from the 1970s until the beginning of the 21st century- can be described as the period of taking international initiatives and countermeasures to stop the exploitation of privacy. Additionally, it is when the Internet[13] was starting to become more and more mainstream. In regards to the first aspect of this period, several international and national efforts were taken such as, but not limited to, Fair information Principles of 1973, the U.S. Privacy Act of 1974, the OECD Guidelines of 1980, The Council of Europe's Convention 108 on Data Protection of 1985, leading up to the European Data Protection Directive 95/46/EC of 1995, and the Charter of Fundamental Human Rights of 2000. These guidelines, conventions, directives, regulations, and charters all acknowledged the importance of privacy as a human right that must be protected. The fourth and final period began with the start of the 21st century. It is defined by the events of 9/11 in the U.S., the extensive use of the Internet, and IT integration. The importance of 9/11 in this context is that it added a deeper meaning to privacy and how the acquisition of information is lethal in the fighting against criminality, fraud, and terrorism. Additionally, the backlash caused by 9/11 and what followed from revelations concerning the U.S. government's mass surveillance programs, showed that regulations were taking back seats for legislation that prioritized law and order. This proved that safeguarding privacy has become a political issue that can't be solved using legal means alone[14]. From this point forward, it became clear that the onward progression of the right to privacy was on diverging paths; one driven by politics, economy, and enhancing consumer experience as displayed by the U.S., and the other motivated by the protection of personal information from any type of misuse as a fundamental human right as perceived by the EU. The second difference maker in this period was that the Internet became mainstream and accessible to almost everyone via IT tools, and later through

[13] The Internet began in 1969 as an experimental network called ARPAnet and was funded by the US Department of Defense to ensure that its computer system would remain functional in the event of an enemy attack that was feared during the Cold War. In the 1980s, the National Science Foundation (NSF), the scientific and technical agency of the United States Federal government expanded ARPANET. In 1989, the name "World Wide Web" was invented by Tim Berners- Lee, a British scientist, working at the European Center of nuclear research in Geneva. In 1990 the ARPAnet was decommissioned. After that, the rise of popularity of the Internet in the United States coincided with the outsourcing in 1995 of the internet management from NSF to the private sector; at that time the Web had 10,000 servers around the world. See A short history of the Web | CERN (home.cern) and ARPANET | Definition, Map, Cold War, First Message, & History | Britannica visitation date 13/2/2020

[14] Holvast (Jan), OP. Cit. supra note 7, page 39

search engines and social media platforms. The Internet, alongside IT tools and globalization, created new challenges for information privacy. These creations developed a parallel reality to the physical world in which it is borderless, and information can be instantaneously exchanged. The integration of information with technology gave rise to the term "data". Consequently, individuals had to be worried about the protection of their information and privacy in the physical world, and the virtual world as well. Thus, privacy became an issue in the digital world and the notion of "e-privacy" began to take shape. In that sense, the internet can be depicted as "Janus"[15] or double-faced. It provides an excess of information for everyone, eases complex tasks, facilitates daily lives, and offers anonymity and the perception of freedom. However, it also stores every possible action regardless of whether it's significant or not. It transitioned from a simple facilitator or a tool for getting tasks done to an indispensable extension of ourselves. As captured by Edward R. Tufte, "There are only two industries which refer to their customers as users, drugs, and computers". Additionally, public and private entities exploited this form of addiction and realized that the internet allows for an easy, fast, efficient, inexpensive, and detailed collection and mining of information that can be used for marketing and other purposes that have value and generate economic profits. Consequently, personal information has been collected online through search engines, websites, social media platforms, network advertisers, and from phones, cars, or any smart object found in possession or utilized by an individual directly or indirectly. These actions coupled with the capabilities of IT tools have damaged the privacy of individuals in the virtual world and impacted their actual reality. Moreover, it has caused the deterioration of people's trust in the online environment. In that sense, personal privacy and the Internet economy can't mutually coexist without effective restrictions and compromises.

From the perspective of an individual's national and international security, there is an important distinction to be made between the era before cyberspace and that which we live in now. Before digitalization and the excessive use of the internet and its tools, the nature of weapons, the nations that possessed those weapons and their destructive capabilities were known. Additionally, there was a distinction between times of peace and war. However, cyberspace has changed this reality. Cyberspace is omnipresent but it is not menacing; the

[15] In ancient Roman religion and myth, Janus is the god of beginnings, gates, transitions, time, duality, doorways, passages, frames, and endings. He is usually depicted as having two faces.

danger it yields lies in its utilization methods. Accordingly, it revolutionized the notion of war and created inconceivable ways of expressing power and dominance. Thus, the assessment of a nation's power stopped being solely measured through a combination of manpower, machinery, equipment, geographical advantages, and strong self-esteem. It became a matter of obtaining crucial information and using that information to cripple other countries through technical skills, surveillance programs, and advanced technologies. Intelligence agencies became the determining factor in showcasing a nation's strength in cyberwarfare. Moreover, with technologies that operate in cyberspace such as laptops, cameras, smartphones, electric cars, and other smart devices in every home and on every street; it became easy to tap in and access these devices to wreak havoc and cripple entire systems. Furthermore, the fact that it is much easier to initiate cyberattacks than to defend against them, coupled with their untraceable nature would give grounds for plausible deniability that increases their impact. Hence, periods of peace and war have become indistinguishable, and the way regulatory systems are set up made them inefficient in dealing with the threats of cyberspace[16]. Therefore, it became a matter of procuring cybersafety rather than just cybersecurity

From a societal perspective, it was believed that this period would propel mankind's drive toward the fulfillment of freedom since they would have the ability to freely acquire and globally share information available at their fingertips. However, the missing piece in the aforementioned proposition is that the human mind isn't just dependent on information; rather it can be broken down into three elements: information, knowledge, and wisdom. The Internet and IT tools greatly facilitated the acquisition, transmission, preservation, and retrieval of information. It also continues to speed up normal and complex functions, and offer instantaneous solutions to problems. However, it is argued that excess information may counterintuitively prevent the attainment of knowledge and suppress the procurement of wisdom. The reasons behind this rebuttal are that the abundance of information in circulation has eroded its sense of significance and removed a key feature that was once ingrained in our society which combines substance and aesthetics to provide a better medium for attaining true knowledge. Additionally, knowledge was attained through physical interactions that added an emotional and psychological dimension to the exchange of facts. Nowadays, the incalculable number of information presented to each one

[16] Kissinger (Henry), OP. Cit. supra note 1, pages 343-345

of us in every waking moment, coupled with the ease of attainment has resulted in accepting such information as facts at face value. However, facts are misused or misunderstood in that context, since they are rarely self-explanatory. The significance and interpretation of facts depend on assigning them to certain frameworks, perceiving them in different contexts, and their relevance to a specific time and place. Accordingly, with the increase in society's perception of facts and information, the relation between problems and solutions becomes clearer and more attainable. In other words, societies and policymakers are under the pretense that every question has a readily available answer which only requires to be "looked up" rather than thought through and perceived in a broader context of experience and history. Thus, the absence of perspective with the abundance of information has rendered actual knowledge and wisdom as rarities. Hence, it may prompt policymakers to be reactive in finding answers to issues; perceive them as singular isolated events rather than reflecting and acknowledging them as part of a wider scale as demonstrated through history, and proactively dealing with them[17].

The preview of history's four periods shows that privacy evolved from a feeling or perception; to a virtue that must be guarded against from physical trespass and connected to a home; to a right coined as "the right to privacy" which protected against tangible and intangible violations and acknowledged as a fundamental human right by directives, guidelines, and regulations; to an intertwined entity with "data" in the virtual world dubbed as e-privacy, and safeguarded by data protection regulations. It also shows how privacy went from a right to a commodity worth exploiting, trading, and selling, and from a personal issue to a political advantage for governments to control. This resulted in rendering personal protection secondary in the context of global dominance, which created a rift between countries' perceptions and priorities in relation to data and conducting foreign affairs (i.e., EU/U.S.). Meanwhile, policymakers and regulators went from total negligence to proper acknowledgment, but then have fallen victims to the reality of the situation, since the cyberworld with its ICT tools are developing faster than regulations and at the same time the quality of regulations deteriorated and became reactive, inadequate, and tailored to specific needs and times absent knowledge and wisdom. Nonetheless, the year 2018 marked the adoption of the General Data Protection Regulation (GDPR) by the EU, which is deemed as a revolutionary regulation with the capability of protecting data and

[17] Ibid, pages 348-352

privacy in the virtual world with its borderless nature, global influence, and massive fines. For this reason, a major portion of this thesis will be dedicated to studying the different aspects and international impact of this regulation.

Parallel to the unfoldment of privacy, the internet, and cyberspace over time, another field that was influenced by these developments and could potentially provide the needed remedies for the problems they present was progressing as well. This sector is the extra-judicial system of dispute resolution or Alternative Dispute Resolution methods.

Disputes and humans go hand in hand; one can't exist without the other. The inevitability of disputes can be attributed to the fact that no two humans are the same. Accordingly, there have always been differences in interests, goals, and perspectives that positioned humans on an unavoidable collision course; whether in early tribal days over food, shelter, and mates or in recent documented history over family matters, commercial transactions in the real or virtual world. Thus, preventing conflicts from ever occurring is a fruitless endeavor. However, people have always found ways in which they can resolve their disputes. For this reason, the notion of ADR, although it wasn't labeled as such, has always concurred with human disputes, predating judicial systems. The earliest citation of actual ADR methods can be traced back to 1800 B.C. in the Mari Kingdom (in modern Syria) that used mediation and arbitration in disputes with other kingdoms[18]. But, as time passed, the primary way of settling conflicts became through courts. This can be attributed to the minute number, and nature of disputes that were confined to the boundaries of small societies. Nonetheless, as humanity evolved, so did the number and nature of their conflicts. Accordingly, the efficiency of courts dropped as a result of the diverse nature of disputes that had complex cultural and physical elements acquired through the varying types of interactions and relationships. Thus, ADR methods were back in the spotlight. Moreover, due to the ease of global communications which bridged distances, the need for these methods grew. Hence, negotiation, mediation, and arbitration became the favorable means of resolving disputes, especially in commerce. Although these methods weren't perfect, their advantages outshined their disadvantages, particularly in commercial disputes where traits such as confidentiality, flexibility, party autonomy, and time and cost-saving appealed to the seekers of extra-judicial

[18] Jerome T. Barrett, Joseph P. Barrett, A History of Alternative Dispute Resolution: The Story of a Political, Cultural, and Social Movement, published in Affiliation with The Association For Conflict Resolution, August 2004, ADR Timeline pages xxv-xxx

mechanisms. The human perception in these situations (i.e., commercial disputes) shifted from trying to terminate relationships and exit as either winners or losers; to trying to reach compromises, preserving relations for future benefits, bridging differences, and securing a win-win outcome. Accordingly, the essence of dispute resolution methods proved to be beneficial in efficiently resolving different issues across different eras. The 1970s mark an important period in recent history where Europe and North America witnessed a significant increase in civil court cases. This event drove scholars and lawyers to label this occurrence as a "litigation explosion"[19], which encouraged the exploration and utilization of ADR. Accordingly, the modern ADR movement began, in which ADR gained tremendous exposure and the caseload for ADR methods increased dramatically. Moreover, it became a field of study and allowed for its professionalization and expansion. However, since it is not feasible to study every ADR method in the context of digitalization, this thesis will focus on Arbitration.

Arbitration is an extra-judicial dispute resolution mechanism recognized by law. It was created by merchants thousands of years ago, which dubs it as the oldest and most quarrelsome alternative dispute resolution method[20]. Its growth and importance throughout several decades can be attributed to the role it played in economic life, specifically in international trade. Additionally, globalization and the complex nature of international trades proposed several obstacles for judicial systems. However, the demands of trade always prevailed over its obstacles. Thus, it had to resort to means that facilitated its operations and preserved the exchange of benefits. Hence, due to the uniqueness of arbitration in regards to its confidentiality, flexibility, party autonomy, international recognition and enforcement power of its awards, and to some extent its time and cost-saving attributes; it became the go-to method to resolve disputes arising from international trade and business transactions.

On a more technical level, arbitration can be described as a procedure initiated based on the decision of conflicting parties who submit the resolution of their current or future dispute to

[19] Marc Galanter, The Day After the Litigation Explosion, Article 4, published in Maryland Law Review, Volume 46, No. 3, Issue 1, 1986, pages 3-5, found at https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2633&context=mlr visitation date 14/2/2020

[20] Derek Roebuck, Cleopatra Compromised: Arbitration in Egypt in the First Century BC, Journal of the Chartered Institute of Arbitrators, Volume 74, Issue 3, August 2008, pp. 263-268, page used 263, According to this author, both private and public arbitration were common in the Egypt of antiquity and both started with attempts to reach settlements.

neutral and independent third parties (i.e., Arbitrator/ Arbitral Tribunal). Accordingly, arbitrators procure their authority and method of handling disputes from the contractual parties and not from the state. Thus, parties resolve their differences through arbitrators that issue binding awards based on the terms of their agreement following a fair hearing. Therefore, arbitrators can be deemed as private judges per their decision-making authority. The most appealing aspect of arbitration is its dual nature. It combines the specificity of ADR methods which makes it pleasing for disputants and at the same time has the enforcement power of judgments rendered by normal litigation with an international scope secured by the New York Convention in 1958. Hence, it's a fusion between the advantages of judicial and extra-judicial dispute resolution systems, which makes it better in adapting to the ever-changing nature of disputes as a function of both: the linear progression of time and the exponential leap in technology.

The 21st century is witnessing a societal transformation of unperceived magnitude. Physical communications and interactions decreased over the years, as new technologies started to separate people physically but brought them closer virtually. It opened a new medium for communications, interactions, jobs opportunities, and business transactions. Accordingly, the overwhelming integration of information technology tools which interferes in every minute aspect of our daily lives, and the creation of a virtual world altered the old standards of living and manifested new ones. In turn, these circumstances demanded global sectoral adjustments in every field. Thus, entailing the need for an overhaul of the legal framework that governs those sectors, which implies modifying the legal sector as well.

In regards to the nature of disputes, cyberspace created a borderless world with instantaneous communication and obligation fulfillment, in which the laws of traditional disputes didn't apply. Additionally, disputes may arise over subject matters that don't physically exist or could be changed or modified by a push of a button on the other side of the world. Moreover, the biggest revolution in communication's history coupled with the free movement of people, goods, and services, gave virtual transactions an economic value with an impact on the physical world. Consequently, it led to an unescapable formation of online legal relationships that had newly established rights such as the data protection right. The right to data protection is intertwined with the right to privacy which became rigorously regulated in Europe and other parts of the world. Accordingly, these rights were enmeshed in the fabric of e-disputes and influenced how

every single transaction or communication is established, especially since e-commerce became popular and disputes between contractual parties that don't know each other and are in different countries increased. Disputes were mainly about prices, late deliveries, product defects, certain specifications, and more recently concerning the protection and security of their privacy rights and digital infrastructure. Thus, the internet, e-commerce, e-privacy rights, and online disputes, are coexistent; they reshaped the entire notion of conducting business transactions or forming relationships. The instantaneous initiation and conclusion of online contracts transformed daily lives and dispute resolution into a modern-day digital "drive-through" society accessible from the comfort of homes or handheld devices[21]. Therefore, traditional judicial and extra-judicial dispute resolution methods became unfit and inconvenient to deal with online disputes, since these disputes have demanded higher standards of convenience, efficiency, speed, and money-saving. These traits may have been the difference-makers between traditional judicial and ADR methods, but the virtual nature of disputes exposed new obstacles for traditional ADR mechanisms. However, the traits that have always propelled extra-judicial dispute resolution methods over judicial ones; proved once again crucial in giving them the advantage to adapt and shift from analog to digital means. Thus, the high number of disputes, especially those of low and medium value, coupled with their international elements, constantly evolving nature of technologies involved, and the shift from a localized to a delocalized setting in which the choice of law and determination of jurisdictions became a complex issue; necessitated the formation of a virtual or online dispute resolution system (i.e., ODR). In turn, this also propelled the initiation of cybersecurity countermeasures that would mitigate the threats of cybercrime which in turn can cripple the extra-judicial industry, cause distrust in its integrity, and reveal crucial information and secrets.

Last but not least, this era has revealed an inseparable correlation between online commerce, data protection, data security and privacy rights, online dispute resolution methods, and the daily lives of people. The confluence of these manifestations has presented consequences, problems, and at the same time offered remedies for these difficulties. In other words, it tested the foundations of our critical infrastructures, belief system and challenged the integrity of our

[21] Amy J. Schmitz, 'Drive-Thru' Arbitration in the Digital Age: Empowering Consumers Through Binding ODR, published in Baylor Law Review, Volume 62 Issue 1, 2010, pp. 178- 244, pages used 179-182, found at https://core.ac.uk/download/pdf/217048178.pdf visitation date 15/2/2020

traditional litigation systems, while paving the way for ingenuities in acclimating with cyberspace. For all the above reasons, the second part of the thesis will focus on both sides of the digital era by showing its influence, issues, problems, and remedies presented to and by alternative dispute resolution methods, especially arbitration.

Finally, to add context and perspective to the aforementioned issues, I must showcase the elements of scientific research that have guided my endeavor in search of academic truths.

Firstly, the purpose of this thesis is to assess the extent of influence caused by digitalization on ADR processes. This will be done through an in-depth exploration and analysis of the transformation caused by the digital age on the perception of legal rights (i.e., right to privacy and data protection), for the digital age has altered how: interactions and legal agreements occur, disputes arise, and contracts drawn up, established, enforced and concluded. Accordingly, one of the ways of achieving this purpose is through examining the most recent and robust data protection regulations in the world today (i.e., the General Data Protection Regulation of the EU). The GDPR has been labeled as the gold standard of data protection regulations and aims to create virtual borders in a borderless world. However, to determine the extent of its influence, it needs to be studied from a national and international perspective, and administered to contractual rights and obligations best showcased in extra-judicial dispute resolution methods. Another area of study that complements the purpose of uncovering the true scale of the impact caused by digitalization is through IT integration and the omnipresence of cyberspace. These issues have presented problems and offered ways of drawing up reasonable remedies that may mitigate the threats of the cyberworld on these institutions such as the ICCA-NYC Bar-CPR Protocol on Cybersecurity. Thus, it is important to study all aspects of digitalization to determine their potency in relation to the ADR process.

Secondly, the importance of exploring the interrelation between digitalization as perceived from data protection regulations, cybercrimes and cybersecurity guidelines, information technology integration, and ADR can be realized through their individual and collective impact on every aspect of our lives. The issues discussed in this thesis formulate a complete cycle of causes and effects or problems and remedies that aren’t just applicable to one sector or domain in a certain timeframe. Moreover, the importance of adjoining these topics shows that the influence of the digital world exceeds its virtual boundaries and directly affects the real world at the macro,

meso, and micro levels of society. Thus, actions taken or not taken in the virtual world have consequences on the actual world. Furthermore, the importance of focusing on ADR methods, especially arbitration goes back to its adaptability and dual nature that presents it as the most effective method of securing rights infringed in or through cyberspace. On the grand scale of things, cyberspace has manifested several changes in regards to international affairs, foreign policies, state sovereignties, electoral campaigns, economies, laws, national policies, etc. In other words, it established a new way of life that has discarded the perks and perils of the traditional one.

Thirdly, the novelty in the thesis can be expressed through the manner in which these topics will be presented. It offers context and perspective in an age where an abundance of information is always available and in circulation, but lacks the depth necessary to provide knowledge. These topics are relatively new and have been the focus of discussions for the past several years in certain parts of the world, especially first-world countries that have been directly affected by digitalization and have functional ADR and ODR systems in place. However, this field is constantly developing and we are still in the early stages of its development. Therefore, there are several ways in which each separate topic can be approached. This dissertation combines the different ways in which these topics meet and the extent of influence that one has over the other. Thus, studying their interrelation and impact in relation to traditional means is like taking a step backward in order to take two steps forward and offer insight into what the future might hold. Additionally, it could serve as a frame of reference in this part of the world that doesn't have an adequate data protection regulation, lacks proper digital access and infrastructure, and still heavily depends on traditional judicial systems and hard copies, rather than shifting towards digital means and normal or online alternative dispute resolution methods.

Fourthly, the difficulties that accompanied the study of this topic can be divided into personal and logistical. The main personal difficulty was in studying a foreign legal system that was entirely different from the local Lebanese one. It required a lot of effort in searching and understanding the workings of foreign laws, especially since some aspects of legal systems are based on cultural and societal norms which differ from one country to another. This difficulty was recognized while analyzing court decisions, since courts would have different interpretations on the same subject, or give certain legal principles broad or narrow scopes of application

depending on the court's discretionary power in relation to the impact of its decisions on multiple societal levels. Although courts in any legal system have discretionary powers, however, the basis and context of these powers are societal and differ from one legal system to another. An additional personal difficulty was applying what was learned from foreign data protection regulations on ADR processes. As of today, the European data protection regulation (GDRP) has no equivalent, especially in a third world country like Lebanon, so other data protection regulations couldn't be used as a frame of reference that would give practical context to data protection and how they influence ADR. Additionally, trying to study different data protection systems for example the one used by U.S. or China to produce a comparative study would have required writing several pages on the backgrounds, motives, priorities, and practical application of their laws to provide context, especially that all three systems immensely differ from one another. That is why it sufficed to study the most advanced regulation (GDPR) and apply it to arbitration only, which too will require exceeding the pre-determined limit of pages allowed for this thesis. Also, this difficulty is enhanced due to the inclusion of IT integration and cyberspace issues. Thus, preserving the richness of the content through integrating several different ideas and regulations will prove to be troublesome. Concerning the logistical difficulties, although there are several writings on these topics independently and few on them jointly; however, almost all required a special type of access and paid subscriptions. Additionally, the lack of availability of hard-copy books, articles, and other references in Lebanon, made the majority of references in this thesis e-references. Moreover, the Covid-19 pandemic and the economic crisis in Lebanon made it extremely difficult to acquire online sources through paying fees in foreign currencies and freely moving from place to place in search of references in local libraries.

Fifthly, this thesis will integrate different types of methodologies that are befitting of the topic. The first part will utilize the descriptive, analytical, and deductive methodologies which are important for transitioning from the general EU data protection framework to the specifics of the GDPR; its implementation, and its integration with ADR. The second part follows a methodological combination of comparative, descriptive, and analytical systems of study. They are tailored around the different issues explored which cover: the comparison between ADR and ODR systems which will highlight their importance; the influence of cyberspace and its ramifications on extra-judicial dispute resolution methods.

Hence, based on the information showcased in the introduction, this thesis will try to answer the following question:

To what extent does the amalgamation of the legal and technical manifestations of global digitalization influence the specificity of ADR methods, especially arbitration?

In pursuit of answering the aforementioned question, this thesis will be divided into two parts. Part 1 will be entirely dedicated to studying data protection and its influence on arbitration, which includes an in-depth analysis of the GDPR with its national and international implementation and its integration with the process of arbitration. Whereas, Part 2 will focus on the remaining aspects of digitalization manifested through information technology which yielded the need for online dispute resolution procedures. In addition to cyberspace and its consequences on ADR, with the proposed remedies.

PART 1: Data Protection: A Multifaceted Response to E-Privacy Violations

Universally, "Data Protection" is defined as a procedure carried out by specific individuals or entities that aims to ensure the safeguard of private personal information from distortion, compromise, loss, or public broadcasting without prior consent or awareness in a transparent manner. It has become commonly acknowledged that private entities and governments around the world have repeatedly shown their unmatched capabilities to collect, mine, keep, and share personal information without disclosing these activities to data subjects unless rules restricting their actions are in place[1]. Accordingly, data protection law-now unanimously known- is the law designed to control the use of personal information.

For this delicate and sophisticated process to reach a high level of viability away from any circumvention, it had to be legally codified and rigorously enforced. Proper implementation of data protection laws -on a national and international level- binding individuals, small businesses, companies, and more importantly state and state sectors, is a leap forward in the preservation of privacy rights.

Over the course of the last half-century, nations around the world witnessed the interconnection between privacy- as a fundamental human right- and data protection. As the years went by, and as data took on several forms and had multiple branches that proliferated rapidly, it became clear that the two rights are deeply intertwined in such a way that a violation of one of these rights directly influences the other. This phenomenon, coupled with the rise of globalization and the borderless nature of the internet, created conflicts concerning the traditional jurisdictional principles and complexities in global implementation. Thus, national and international lawmakers were caught off guard. Accordingly, the regulation of data protection has become an exercise of power which turned it into a global race or competition. Internationally, the concept of data protection stemmed from the same roots (i.e., protecting privacy), but diverged due to different priorities, incentives, legal systems, beliefs, and the politicization of the subject. The discrepancies in approaching data protection caused

[1] Privacy International, A Guide for Policy Engagement on Data Protection, Part 1: Data Protection Explained, published September 2018, page 1, found at https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf visitation date 1/2/2020

unavoidable collisions on the international stage between the EU and the U.S. Consequently, since the U.S. doesn't have a specified regulation for the sole purpose of data protection; the focus of this part will be on the EUs' data protection regulation. Thus, (CHAPTER 1) will cover the regulatory framework of data protection in Europe which has a global reach, and (CHAPTER 2) will present a theoretical and practical study of the influence of the GDPR on judicial and extra-judicial processes.

CHAPTER 1: The Regulatory Framework of Data Protection

When studying a regulatory framework in a certain legal field, we are looking at an omnibus of hierarchical standards outlined in an almost sacred order. These standards slightly differ from one country to another but are similar in essence. It's inevitable, especially in a new regulatory framework such as "Data Protection Laws" to witness several modifications, amendments, and frictions between multiple sources of law that either collide or jointly figure out an agreed-upon course of action to tackle this subject. Leading up to the adoption of the GDPR in 2018, it has been demonstrated that different countries approach and regulate data protection from different positions. A manifestation of this premise could be induced from (Sub-Chapter 1) that will be dedicated to a theoretical and practical overview of the general approach used to protect data in the EU that led to international complications with the U.S. Whereas, (Sub-Chapter2) will be a study of the national and international enforcement mechanisms set forth by the GDPR.

SUB-CHAPTER 1: The European Model of Data Protection

As mentioned, since the EU has the most conclusive data protection regulation that has national and international reach, the focus throughout the following two chapters will be on its regulatory framework. Accordingly, it is best to methodically showcase the approach adopted by the EU in a theoretical overview of the components that formulated the GDPR (Section 1), and a practical review of the landmark case that reaffirmed the position of the EU and further exposed the rift between the EU and the U.S. concerning the subject of data protection (Section 2).

Before commencing with the study, there are some common terms expressed similarly in each of the following regulations that should be clarified to provide a better understanding of the issue at hand. The following definitions are mentioned in the EU's GDPR Article 4[2] :

1. Data Subject: Any natural or legal person who is the subject/owner of the data in question.
2. Personal Data: Information that identifies or is used to identify- labeled as identifiable information-a data subject whether directly or indirectly.
3. Processing: Operations performed on personal data ranging from collection, organization, storage, recording, retrieval to destruction by dissemination, erasure, blocking or even, transmission via broadcasting, disclosure, adaptation, consultation, alignment, or combination. The broadness of this definition aims to cover almost all activities related to personal data.
4. Controller: Any natural, juristic person whether private agency or public authority, bound by national or community laws or regulations that determine the purpose of processing.
5. Processor: Any person or entity responsible for the processing operation on behalf, or designated by the controller.
6. Recipient: The receivers of personal information. However, authorities receiving personal data as part of a specific inquiry will not be deemed as recipients.

[2] Regulation (EU) 2016/679 of the European Parliament and 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- The General Data Protection Regulation (GDPR), Official Journal of the European Union, No. L 119/1, 4/5/2016 (hereinafter referred to as General Data Protection Regulation or GDPR) Article 4, found at https://eur-lex.europa.eu/eli/reg/2016/679/oj visitation date 2/2/2020

7. Establishment: A controller who carries out processing assignments through fixed arrangements with member states
8. Sensitive Data: Personal data that reveals the racial or ethnic origin, political orientation, religious or philosophical convictions, or memberships in trade unions. Additionally, biometric or generic data processed to gain specified identification of a natural person. In addition to health data or a person's sexual tendencies[3].

SECTION 1: The European Union's Building Blocks of Data Protection

Data protection isn't a new concept. It has been a work in process for almost 80 years now. As mentioned in the introduction, the idea of data protection is a byproduct of the right to privacy, since protecting privacy in the digital age can't be achieved if data isn't protected. Accordingly, with Europe being an advocate of prioritizing the protection of human rights, it approached data protection in the same manner. Data protection in Europe can be traced back to 1957 in Article 16 of the Treaty on the Functioning of the European Union (also known as The Treaty of Rome). It recognized that the protection of personal data is a universal right and that it's the job of the European Parliament and the Council, abiding by regular legislative procedures, to set down rules on the processing and regulation of free movement of personal data by every sector of the EU (bodies, institutions, agencies, offices) and member states when performing activities within the confines of Union law[4]. The first stepping stone in the EU's journey to regulate data protection started indirectly in 1973 when the fair information practices were established in a collective effort between different U.S. federal sectors. These practices portrayed the proper ways in which information-based societies deal with handling, storing, and managing information while preserving fairness, privacy, and security[5]. Consequently, they paved for an

[3] Ibid, Article 9
[4] Treat on the functioning of the European Union (TFEU), 1957, Article 16, Found at https://www.jus.uio.no/english/services/library/treaties/09/9-01/tfeu_cons.xml#:~:text=The%20Union%20shall%20have%20competence%2C%20in%20accordance%20with%20the%20provisions,of%20a%20common%20defence%20policy.
[5] Privacy Act of 1974, Pub. L. No 93-579, 88 Stat. 1896 (Dec. 31, 1974), codified at 5 U.S.C. §552a (1974), The Fair Information Practices Principles, Found at https://itlaw.wikia.org/wiki/Fair_Information_Practice_Principles visitation date 20/5/2020

international convention to adopt the notion of data protection which resulted in the Guidelines of the Organization for Economic Cooperation and Development (OECD) in 1980. These guidelines used fair information practices' core values to establish eight principles that were rectified and codified by member states. These principles are: the collection limitation principle, data quality principle, purpose specification principle, use limitation principle, security safeguard principle, openness principle, individual participation principle, and accountability principle[6]. Parallel to the admittance of data protection principles in the OECD guidelines, the European Convention on the Protection of Human Rights and Fundamental Freedoms (ECHR) was the first European Convention to realize data protection. This was achieved through Article 8 of the ECHR which provided a personal entitlement to privacy and protected from infringements and violations that confined the enjoyment of such right unless authorized by public authorities under certain stipulations[7]. Consequently, as time went by, changes had to be made to this right which involved including the protection of data as a right accompanied with the protection of private life. After that, the 1980s in Europe marked the establishment of the Council of Europe's Convention 108 on Data Protection to protect the fundamental rights and freedoms related to data subjects' personal data through protecting and preserving their right to privacy[8]. It served as the first legally binding international instrument for the protection of individuals' data against any maltreatment that occurs through processing, collection, or even transmission, whether locally or internationally. Additionally, it tackled issues related to restrictions on the processing of sensitive data and introduced rights to data subjects that would allow them access to their personal data and decide whether they like to change them or not[9].

The 1990s marked the beginning of significant leaps in data protection in the EU. This feat was achieved through the adoption of the European Data Protection Directive[10] in 1995 (95/46/EC).

---

[6] The OECD Privacy Guidelines, 2011, page 21, found at https://www.oecd.org/sti/ieconomy/49710223.pdf visitation date 4/2/2021

[7] European Convention on Human Rights, Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Strasbourg, October 2, 2013 Article 8, page 11, found at https://www.echr.coe.int/Documents/Convention_ENG.pdf visitation date 12/24/2019.

[8] Ibid, Article 1, found at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 visitation date 1/15/2020

[9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 1/10/1985, found at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 visitation date 20/5/2020.

[10] Definition of Directive: "a legislative Act of the European Union produced by the Council of the European Union and the Commission of the European Union. It directs member states to produce a certain effect within a certain

The main purpose of the Directive was to propose a safeguarding measure of unified laws against the processing of personal data related to data subjects. It also allowed for a secure free flow of data across member states[11] by implementing its three principles which revolve around: *transparency* by providing data subjects with information regarding the processing of their own data which guarantees the fairness of the operation[12] and processing for a *legitimate purpose* in a lawful environment[13] while respecting a *proportionality* standard between the primary cause for processing and data used for a specific operation, and later getting rid of data which no longer serves their purpose with exceptions regarding processing for statistical, historical or analytical means[14]. Moreover, extensive restrictions apply when the personal data is classified as "sensitive data" requiring more explicit consent[15]. Furthermore, this Directive established Working Parting 29 (WP29), which was an independent European Union Advisory Body concerned with the protection of individuals with regards to the processing of personal data. It was made up of EU state representatives, an EU data protection supervisor, and a representative of the European Commission. It was tasked with giving advice, providing opinions, consultations, and recommendations on subjects related to privacy, the protection of data, and its free flow in the EU and internationally across borders. Following that, several other specialized directives came into fruition some of which were: Specialized Directives in the Communications Sector: 97/66/EC (concerning telecommunication) amended by Directive 2002/58/EC (concerning electronic communication, also known as ePrivacy Directive) later amended by Directive 2009/136/EC. The striking concern about all these directives that tried to deal with data protection in the communications sector and other related fields is that they were almost always one step behind the initiators of such technologies. In other words, they were blindsided by the magnitude and impact that the revelations in communications brought to the world. Thus, they

time. This achieves the Community goal while respecting national differences. The member state need not legislate if it can achieve the same result by administrative measures. Failure to comply can result in action before the Court of Justice of the European Union at the instigation of the Commission. Directives are not directly applicable but they can have a direct effect. Found at Collins Dictionary of Law, Ed. 3, 2006

[11] 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, Official Journal of the European Communities, No L 281/31, 23/11/1995, page 1, preamble paragraph (4-5-6) can be found at https://eur-lex.europa.eu/eli/dir/1995/46/oj visitation date 23/1/2020

[12] Ibid, Articles 10-11

[13] Ibid, Article 6(a)

[14] Ibid, Article 6(b)

[15] Ibid, Article 8

left multiple loopholes ready for exploitation, whether it was in social media, online profiling, applications on smartphones, or the unstoppable widespread of the internet in general. Also, the implementation of these directives by member states wasn't optimal and left room for maneuvering which caused the fragmentation of the directives diminishing their purposes[16].

It is noteworthy to mention that actions taken by the European Union from 1993 till 2009 were based on the three-pillar structure[17]. They were done through treaties that were adopted and voted on democratically and voluntarily by member states. Accordingly, with the EU being based on the rule of law and treaties being the source of law between member states, treaties were significantly important with binding powers among member states. Additionally, the Charter of Fundamental Human Rights was proclaimed in the year 2000 in the Nice summit and aimed to combine the rights of individuals of European Union member states that were scattered among several Treaties and Conventions under one main source of law. Article 7 of this Charter amended Article 8 of the European Convention on Human Rights (Convention 108) by replacing the word correspondence with communications when describing the right to respect privacy. Also, Article 8 was titled "Protection of Personal Data" which explicitly addressed the right of personal data protection upon fair processing with prior consent, and a right of access to this data from data subjects supervised and controlled by an independent authority[18]. However, this charter wasn't given its legal status until 2009 with the adoption of the Lisbon treaty.

The Treaty of Lisbon marked the beginning of a new era for the European Union on many different levels. It is considered to be a "reform or constitutional" treaty amending both the Treaty of the European Union and the Treaty establishing the European Community[19]. It gave

---

[16] Electronic Privacy Information Center, Article," EU Privacy and Electronic Communications (e-Privacy Directive)" found at https://epic.org/international/eu_privacy_and_electronic_comm.html visitation date 5/2/2020

[17] The 3 pillars from 1993 till 2009 were: the internal market legal basis of the European Community, common foreign and the security policy and judicial cooperation in criminal matters, and the police. See Peter Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", Article, September 2014, page 14 found at: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf visitation date 15/1/2020

[18] Charter of Fundamental Rights of the European Union, published in the Official Journal of the European Communities, C 364/1, 18/12/2000, Article 7-8 found at https://www.europarl.europa.eu/charter/pdf/text_en.pdf visitation date 15/1/2020

[19] Electronic Privacy Information Center, The Lisbon Treaty and Privacy, Article, No date, found at https://epic.org/privacy/intl/lisbon_treaty.html#:~:text=Under%20the%20Lisbon%20Treaty%2C%20the,recognized%20as%20a%20fundamental%20right.&text=%22As%20a%20consequence%2C%22%20he,by%20individuals%20is%20not%20unlimited. visitation date 5/10/2020

the Charter of Fundamental Rights a binding status to render it on par with Treaties. This meant that Articles 7 and 8 of the Charter that explicitly addressed data protection became binding. Moreover, since the right to data protection was also covered in TFEU Article 16(1) as part of the EU's general principles, it dictated important parts of Directive 95/46/EC that became level with the EU's primary law. Thus, it made this right directly and explicitly applicable in a court of law invoked by any person[20]. This treaty also reshaped the way decisions were made by diminishing the three pillars of structure and adopting a proven Community method for decision making instead. This new system worked on the third pillar's data protection legislation that came as solo Council practice, which now required different methods of voting and adoption[21]. The combination of all these different sources of law lead to the creation of the GDPR which is dubbed as the gold standard in data protection and will be the main focus of this chapter.

The General Data Protection Regulation[22] (GDPR) is the latest and most important regulation in the data protection field. It became the standard that must be met by other countries around the world. It developed, reinforced, and improved aspects of previous directives such as, but not limited to, the newly added requirements and purposes for the appointment of a Data Protection Officer (DPO) by controllers and processors[23], the 'one-stop shop' regulation for controllers that work in several EU countries[24], and organized the competence of the lead supervisory Data Protection Authority (DPA) in several ways[25]. Secondly, it expanded the scope of application territorially and extra-territorially based on factors such as the establishment principle, and the

[20] Daniel Cooper, Henriette Tielemans, and David Fink of Covington & Burling LLP Privacy and Data Protection Practice Group, Article, The Lisbon Treaty and data protection: What's next for Europe's privacy rules? published in the Privacy Advisor- International Association of Privacy Professionals, January- February 2010, page 17 found at https://www.cov.com/en/news-and-insights/insights/2010/02/the-lisbon-treaty-and-data-protection-whats-next-for-europes-privacy-rules visitation date 5/10/2020

[21] Hustinx (Peter), Op. Cit. supra note 17, pages 18-19

[22] Definition of Regulation:" A rule of order having the force of law, prescribed by a superior or competent authority, relating to the actions of those under the authority's control".
In Europe: "a form of Act of the EUROPEAN UNION that has general application. A regulation, unlike a decision, applies to more than an identifiable or defined limited number of persons. It is binding in its entirety, unlike a directive, which simply sets out the aim to be achieved. It is directly applicable and does not require to be subsequently enacted in a Member State. It can also have a direct effect". West's Encyclopedia of American Law, Edition 2, (2008)

[23] GDPR, OP. Cit. supra note 2, Article 56

[24] Ibid, Recital 127,128

[25] Ibid, Articles 55, 56, 57

place of contract performance[26]. Additionally, it modified the principles of processing[27], data profiling issues whether manual or automated[28] and set forth a much-improved adequacy protocol that governed cross-border data transfers[29]. Also, it addressed and modified some rights for both sides of the process (controllers and data subjects) such as the right of erasure - previously known as the right to be forgotten[30]-, and emphasized data accessibility and notification rights of data subjects[31]. Furthermore, it streamlined how consent is given and can be revoked[32]; in addition to developing standardized information policies that provide extensive information to data subjects regarding the processing of their personal data and gave them the power to file complaints through private rights of action and class actions to DPA to initiate legal proceedings[33]. Moreover, the European Commission is authorized to adopt delegated acts for setting fixed information as model information icons, and set the procedure of reaching those standardized icons, under this Regulation[34] Lastly, it replaced WP29 with the European Data Protection Board (EDPB)[35].

This summarized overview of the timeline of formulation of data protection in the EU from its early acknowledgment in 1957 to practical actions in the 1970s until the most recent data protection regulation of 2018 (GDPR), is an indicator of how they foresaw the importance of this topic, and directly linked the proliferation of the digital world to basic human rights that would be bound for exploitation, thus in need of protection. For this reason, Europe is considered a pioneer in this field and aims to uphold its status and reputation as a protector of human rights. However, a rigoristic approach of such magnitude at this time where few other countries share the same capabilities, views, and values could render them as outcasts, which in turn will limit their ability to do business and allow for unwelcomed complexities in the judicial system. In a world where countries are dependent on each other for resources of every kind, and where people

[26] Ibid, Article 3
[27] Ibid, Articles 5-11
[28] Ibid, Article 22
[29] Ibid, Article 45
[30] Ibid, Article 17
[31] Ibid, Article 19, 33
[32] Ibid, Article 7
[33] Ibid, Article 12, Recital 143
[34] Ibid, Article 12(8)
[35] Ibid, Article 68

and information travel with ease across countries, being independent in such a crucial area that is shaping up the entirety of our future will lead to conflicts.

SECTION 2: The International Dilemma of Data Protection

The rise of huge multi-national companies that transfer data from one country to another has become a norm in the digital age. Most big data companies are based in the U.S. and have establishments all over Europe, which means that data in large quantities is constantly moving from one jurisdiction to another. Thus, the regulation of international data transfer between countries has become an integral part of every country's regulatory setup. Some nations are driven by protecting fundamental rights (EU), others by preserving trade revenues, international relations, and a free flow of information (US), while others prioritize security (China). This serves as an indicator of the superiority of national laws in a field stimulated by a competitive nature. It is also crucial in protecting the integrity of the regulations and standards set by each national law. More importantly, regulating cross-border data transfers in the modern technological age is vital in safeguarding people's personal information and privacy rights and promoting e-commerce which has become a focal point in the modern economy.

In the U.S., unlike the European Union, the essence of data protection and privacy is mainly dependent on consumer rights and competition preservation. This is achieved through actions taken by the judiciary system and the legislature[36]; supplemented with the role of the Federal Trade Commission (FTC) – as the primary enforcer of data protection in the U.S.-, Federal Communications Commission (FCC), Securities and Exchange Commission (SEC) and departments of health, education and banking. In turn, it has diminished the value of privacy and data protection as fundamental rights as seen in Europe. The American regulatory framework is considered to be a patchwork quilt of different regulations composed from and applied through sectoral laws at the federal and state level making it extremely dynamic, flexible, and robust with a non-prescriptive nature. It is also sustained by private litigation and post hoc governmental

[36] Viviane Reding, The Debate on Privacy and Security Over the Network: Regulation and Markets, Article, published by Ariel and Fundación Telefónica, volume 36, printed in Spain October 2012, Executive Summary pp. 13-14, found at https://lirias.kuleuven.be/retrieve/226688 visitation date 12/2/2020.

enforcement that can arise as compensation due to damages caused by a breach of privacy or unfair business practices, hence interdicting the "precautionary principle" as a means of protecting privacy[37]. Accordingly, the different incentives, beliefs, priorities, and application systems adopted by the U.S. in the data protection field, coupled with an absence of a specialized and independent regulatory enforcement body such as the Data Protection Authority (DPA) in Europe, resulted in the U.S. not having an adequacy decision that would allow for the legal transfer of data between countries. However, this didn't mean the end of cross-border trade between EU-U.S., especially since the U.S. was the leading trading partner of the EU. Thus, an international co-regulatory agreement "Safe Harbor" was established on July 25, 2000[38]. This agreement preserved the EU-U.S. trade partnership and the privacy framework of the U.S. while constituting an adequate basis for cross-border data transfer between the two. The following depiction of the contractual agreements between the EU and U.S. for cross-border transfers serves as a reaffirmation of the firm position and the seriousness that the EU has in regards to data protection. Additionally, it showcases a practical translation of the EU's data protection regulatory system on an international scale and exposes the rift that these two communities have when it comes to the notion of data protection.

Sub-Section 1: The Rise and Fall of the Safe Harbor Agreement

A- Definition of The Safe Harbor Agreement

The Safe Harbor agreement was designed as an optional self-certification program with data protection principles already acknowledged by the EU. It regulated data protection and privacy in the private sector's transatlantic flow of data[39]. This agreement applied to companies and

[37] Alan C. Raul, Frances E. Fairloth and Vivek K. Mohan, The Privacy, Data Protection and Cybersecurity Law Review, edited by Alan Charles Raul published by Gideo Roberton, Fourth Edition, UK, Business Research LTD London, December 2017, Chapter 27(United States), page 364,365

[38] Commission Decision 2000/520/EC, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, published in the Official Journal of the European Communities, L 215, 25/8/2000, found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=en visitation date 15/2/2020

[39] Ioanna Tourkochoriti, The Transatlantic Flow of Data and the National Security Exception in the European Privacy Regulation: In Search For Legal Protection Against Surveillance, Article, published by Penn Law: Legal Scholarship

organizations in the U.S. that received personal data from the EU[40]. Admittance to the Safe Harbor agreement was done voluntarily through signing up for it by informing the U.S Department of Commerce, and it was subjected to annual resubmission. Since the Federal Trade Commission is responsible for the enforcement of data protection and privacy regulations in the U.S., companies that fall outside its sphere of application weren't included in Safe Harbor. For example, financial services and telecommunications industries were excluded, while internet and computer companies, pharmaceutical industries, and a wide selection of companies that provide services such as credit card, healthcare, travel, and tourism services which are also utilized in the EU's internal market were included[41]. Over 4000 companies became part of the Safe-harbor agreement.

B- The Downfall of Safe Harbor and its Implication on Transatlantic Data Transfers

The demise of Safe Harbor could be initially attributed to the omission of limiting national security access by both: The Safe Harbor principles and the European Commission's adequacy decisions[42]. This matter was ignited through two major events: Edward Snowden's Revelations and the *Max Schrems v. Facebook* case.

a) The revelations of secret surveillance by Edward Snowden

On June 5, 2013, reports broke out revealing that the U.S. government through the NSA (National Security Agency) had been collecting millions of American telephone records of Verizon, and after the September 11 attack, it was authorized to implement a program of collecting domestic telephone, internet and email records in bulk[43]. Additionally, U.S.

Repository, Volume 36:2, 2015, pp.459-524, written 4/17/2015, page used 470, found at https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1891&context=jil visitation date 13/6/2020

[40] Ibid

[41] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM/2013/0847 final, November 27, 2013, at 2.2 "The Functioning of the Safe Harbour" found at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013DC0847 visitation date 13/6/2020.

[42] Gabe Maldoff, Omar Tane, Privacy Shield backgrounder, Article, Excerpt taken from "Essential Equivalence and European Adequacy after Schrems: The Canadian Example. Published in Wisconsin International Law Journal, Volume 34, 2016, page 8, found at https://iapp.org/resources/article/privacy-shield-backgrounder/ visitation date 10/6/2020

[43] Ewen Macaskill, Gabriel Dance, NSA Files: Decoded- What the revelations mean for you, Article, published by The Guardian, November 1, 2013, found at

intelligence worked with foreign intelligence agencies on data sharing and surveillance such as in Denmark[44]. Media news outlets such as The Guardian and The Washington Post continued to expose this mass surveillance scheme through information provided by an NSA contractor called Edward Snowden.

Internationally, these reports revealed that surveillance targeted foreign and U.S. communications equally[45]. It was achieved through mainly two programs PRISM and Upstream. In PRISM, companies such as Google, Facebook, Yahoo, Microsoft, AOL, Skype, Paltalk, Apple were forced to turn over communication to and from specified selectors through giving direct access of their serves to the intelligence agency[46]. All of the above allegedly involved multinational data-collecting companies were certified under Safe Harbor. However, such acts were outside the scope of application of Safe Harbor since they fall into the national security exception. Therefore, it crippled data subjects' rights to do anything about the unlawful collection of their data[47].

Meanwhile, the upstream programs are cable-intercept surveillance mechanisms, which provide the NSA with direct access to the data packets moving through national and international fiber optic cables. Allegedly, the NSA alone and in collaboration with telecommunications services copied, stored, and examined communications that crossed the internet such as emails and texts[48].

Although these programs constituted a massive breach of privacy and data protection regulation, they were legalized nationally in the U.S. under the Foreign Intelligence Surveillance

https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 visitation date 18/5/2020

[44] Caleb Chen, The head of Denmark's spy program has been fired for snooping on citizens and lying about it, Article, published on Privacy News Online, August 26, 2020, found at https://www.privateinternetaccess.com/blog/the-head-of-denmarks-spy-program-has-been-fired-for-snooping-on-citizens-and-lying-about-it/ visitation date 10/10/2020

[45] G. Alex Sinha, NSA Surveillance Since 9/11 and the Human Right to Privacy, Article, Loyola Law Review, Volume 59, 2012-2013, pp. 861- 946, page used 929, found at https://dspace.loyno.edu/jspui/bitstream/123456789/121/1/Sinha.pdf visitation date: 18/5/2020

[46] Glenn Greenwald, Ewen MacAskill, NSA Prism program taps into user data of Apple, Google and others, Article, published in The Guardian, June 7, 2013, found at https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data visitation date 18/5/2020

[47] Tourkochoriti (Ioanna), OP. Cit. supra note 39, page 476

[48] Ibid, page 463

Act amended by (USA FREEDOM)[49] in Section 702 and before that Section 215 of the PATRIOT Act[50].

Following these revelations, huge concerns were raised between the EU and U.S., and the public atmosphere regarding the safety and assurances of the Safe Harbor agreement was compromised. This sense of unease was reflected in the numerous investigations and lawsuits against multinational companies alongside a big number of enforcement actions taken by the FTC for violations committed on the Safe Harbor agreement after 2013 which were 29 cases out of 39. These complaints caused the acceleration of the agreement's conclusion[51].

b) Max Schrems v. Facebook (Schrems 1)

In 2011, Max Schrems an Austrian law student formed a non-profit organization to take on Facebook on the grounds of violating European privacy laws. Through his NGO, Schrems lodged 22 complaints against Facebook's head of operations in Europe which is situated in Ireland. These complaints went through the Data Protection Commission (DPC) of Ireland[52].

Two years later, fueled by the revelations of Edward Snowden, Schrems filed another complaint probing whether Facebook was sending his data to the NSA for national security reasons or as part of a cooperation between Facebook and NSA[53]. Moreover, since Facebook was certified under Safe Harbor, he disputed the legality of Safe Harbor based on the national security exception, and whether it was tolerated under the Data Protection Directive and the EU

[49] Uniting and Strengthening America By Fulfilling Rights and Ensuring Effective Discipline Over Monitoring, Act of 2015, Pub L. 114-23, 129 Stat. 268 (June 2, 2015)

[50] Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, (USA PATRIOT ACT) ACT OF 2001, Pub. L 107-56, 115 Stat. 272

[51] Anna Myers, CIPP/US, IAPP Westin Fellow, FTC Enforcement of the U.S.-EU Safe Harbor Framework, Article, no publication date, pages 5-7, found at https://iapp.org/media/pdf/resource_center/IAPP_FTC_SH-enforcement.pdf visitation date: 13/6/2020

[52] Robert Levine, Behind the European Privacy Ruling That's Confounding Silicon Valley, Article, published in The New York Times, on October 9, 2015, found at https://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html visitation date 15/6/2020

[53] Maximilian Schrems, Complaint against Facebook Ireland LTD- 23 "PRISM" to the Data Protection Commissioner, Vienna, June 25, 2013, page 4 found at http://www.europe-v-facebook.org/prism/facebook.pdf visitation date 15/6/2020

Charter of Fundamental Human Rights[54]. However, due to reasons such as lack of evidence regarding his own data being accessed and used, the DPC didn't investigate this complaint[55].

Schrems appealed this refusal to the High Court of Ireland. The court established that although this matter should be dealt with under the Irish law since it consisted a violation of the constitutional right to privacy and freedom, and that further dwelling on the adequacy of the U.S.'s privacy regulations was required pursuant of these virtues[56]. Thus, the Irish law was superseded in this matter by the European Commission's adequacy findings, so it was concluded that the EU law must resume control under Article 25 of the DPD[57]. However, it noted that the prevention to investigate such matters by the DPC under Safe Harbor was overridden by the EU's Charter that expects the EU Commission to guarantee that every data access, even by government authorities is compatible with the EU Charter. Additionally, the U.S. mass surveillance programs that came into light far exceed what was supposedly meant by exempting data access and transfer for national security purposes under Safe Harbor. Hence, this case was referred to the CJEU[58].

The CJEU handled this case on two fronts. First, it addressed the role of the Data Protection Authorities under the Safe Harbor agreement, which confined their independent ability to protect the European citizens' data under Article 3 of Safe Harbor[59]. Second, it took on Safe Harbor's national security exemption, especially after the failure of the Commission's decision to restrict or indicate national or international laws that limit the unrestricted and unmonitored mass surveillance programs used by the U.S [60]. Thus, it considered that these open-ended surveillance

[54] Ibid, page 6
[55] The High Court Judicial Review, Record No. 2013/765 JR, between Maximillian Schrems and Data Protection Commissioner- Statement of Opposition of the Respondent, December 2013, found at http://europe-v-facebook.org/JR_First_Response_DPC.pdf visitation date: 15/6/2020
[56] The High Court, Decision no. 765JR, 2013, between Maximillian Schrems and Data Protection Commissioner, Judgment of Mr. Justice Hogan delivered on the 18th of June, 2014, at paragraphs 52-56 found at http://www.europe-v-facebook.org/hcj.pdf visitation date 15/6/2020
[57] Ibid, paragraph 57
[58] The European Parliamentary Research Service, Fundamental Rights in the European Union: The role of the Charter after the Lisbon Treaty, In-Depth Analysis, March 27, 2015, page 22, found at https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554168/EPRS_IDA(2015)554168_EN.pdf visitation date 16/6/2020
[59] Commission Decision 2000/520/EC, OP. Cit. supra note 38, Article 3
[60] CJEU (Grand Chamber), Judgment of the Court, Case C-362/14, Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, October 6, 2015, paragraph 86, 93 found at http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN visitation date 17/6/2020

schemes disrupt the core values guaranteed by the EU Charter regarding the fundamental right to respect for private life[61]. Therefore, ensuring that adequate protection from third countries was dependent upon guaranteeing an essentially equivalent framework of protection to that enjoyed within the European Union[62].

Hence, on these grounds, and without diving into the substance of the U.S. surveillance laws[63], the CJEU overturned the adequacy decision and struck down Safe-Harbor. This decision was based on Safe Harbors' failure to acknowledge the enormity and implications of the national security legislation which compromised the essence of adequate protection[64].

Although this case is one of high status, magnitude and involves several international entities, however, it could be pointed out that several grey areas were surrounding the application of the law, jurisdictional differences, and lack of efficiency in dealing with such issues. In other words, the timeframe from when Max Schrems initiated the process until its settlement is long and it was draining physically, emotionally, and economically. These issues would have, to some extent, been resolved had they used ADR methods.

Sub-Section 2: The EU-U.S. Privacy Shield

On February 2, 2016, following the invalidation of Safe Harbor, an agreement between the Department of Commerce in the U.S. and the European Commission established the "EU-U.S. Privacy Shield". It was considered as a modified version of the Safe Harbor filling in the gaps that were previously exposed. Although it was found inadequate according to an assessment made by Article 29 Working Party since it failed to cover every aspect of the Schrems decision[65], it was officially approved adequate by the European Commission on July 12, 2016[66].

[61] Ibid, paragraph 94
[62] Ibid, paragraph 74
[63] Ibid, paragraph 98
[64] Ibid, The Final Ruling
[65] Article 29 Data Protection Working Party, WP 238, Opinion 01/2016 on the EU- U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016, page 3, found at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf visitation date 18/6/2020
[66] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 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, published in the Official Journal of the European Union, C 4176, 1/9/2016, found at https://ec.europa.eu/info/sites/info/files/celex_32016d1250_en_txt.pdf visitation date 18/6/2020

The Privacy Shield issued clear limitations on national security access existing in U.S. laws[67]. The restrictive regulations found in it were aided by several U.S. initiatives that addressed this issue such as, the passage of the USA FREEDOM Act that regulated and confined the NSA's bulk telephony metadata program[68], the adoption of the Judicial Redress Act that widened the scope of protection offered by the U.S Privacy act of 1974 to non-U.S. residents with the capability of bringing civil claims against U.S. agencies[69] and the Presidential Policy Directive 28, which came in response to Snowden's revelations; limiting and specifying six purposes that permit bulk international surveillance by federal executive agencies[70]. Also, as a result of the Schrems case, the U.S. State Department agreed on the appointment of an Ombudsperson tasked with investigating complaints by EU residents, regardless of whether they could provide evidence proving access to their own data[71].

Additionally, the Privacy Shield addressed several requirement issues that were omitted by the Safe-Harbor such as, but not limited to, issues related to what should be posted in the privacy policy disclosure list, requirements correlating with onward transfers to controllers and to service providers(sub-processing) which include third-party notifications and limited purposeful processing accompanied by the data subjects' consent and conducting evaluations of service providers, etc. Moreover, the Privacy Shield focused on issues affiliated with data minimization requirements and gave data subjects the right to obtain confirmation of whether an organization has data concerning them. Furthermore, it emphasized the enforcement capabilities of the data subject, through allowing binding arbitration and providing free independent recourse mechanisms. Finally, it gave regulatory oversight jurisdictions to the Department of Commerce requiring organizations to answer their inquiries and requests[72].

---

[67] Ibid, L 207/13 under Access and Use of Personal Data Transferred Under The EU-U.S. Privacy Shield by U.S. public authorities

[68] 114th Congress of the United States of America, USA FREEDOM Act, H.R. 2048, Pub. L 114-24 (2015) found at https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf visitation date 18/6/2020

[69] 114th Congress of the United States of America, Judicial Redress Act of 2015, Pub. L 114-126- Feb 24, 2016, found at https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf visitation date 18/6/2020

[70] The White House, Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities, Policy Directive/ PPD-28, January 17, 2014, Section 2, found at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities visitation date 18/6/2020

[71] Commission Implementing Decision (EU) 2016/1250, OP. Cit. supra note 64, paragraphs 116-121

[72] For a full list of modifications, See: Bryan Cave, A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor", 16,7, 2019 found at https://iapp.org/media/pdf/resource_center/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf visitation date 16/6/2020

However, on July 16, 2020, the CJEU invalidated the Privacy Shield on grounds of inadequate protection under GDPR and the EU Charter of Fundamental Human Rights in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (Schrems II)[73].

The court's decision of invalidity also came as a result of the U.S. surveillance programs that although assessed by the Commission, yet still weren't circumscribed to what is considered as -limited to what is purely essential and proportional- as demanded by the EU law since no clear limitations or guarantees were given concerning their powers or whether they would affect non-US persons[74]. Thus, these actions were considered as violations of Article 52 of the EU Charter of Fundamental Rights. Secondly, the invalidation decision came due to the lack of judicial redress guaranteed to EU citizens. The court decided that the Ombudsperson mechanism wasn't capable of providing a redress body of equivalent protection and assurances similar to the EU law and Article 47 of the EU Charter of Fundamental Human Rights, since there were doubts over the ombudspersons' independence and the rules that authorized them to adopt binding decisions that would impede intelligence services[75]. Finally, the court also ruled in regards to the Standard Contract Clauses, rendering them as a valid means of conducting adequate transfers between EU-U.S. but with additional conditions that will ensure their adequacy[76].

Consequently, with the invalidation of Safe-Harbor and Privacy Shield, the U.S. experience in regards to adopting adequate data protection laws as inscribed by the EU goes back to the negotiation table.

These events have created a perception of fluctuating regulatory environment which added a sense of worrying uncertainty among companies, organizations, and data subjects who were involved whether directly or indirectly in the preceding agreements. Nearly 5,400 U.S. organizations were affected, including several EU-based ones.

[73] Court of Justice of the European Union, Judgement in Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems, Press Release No 91/20, Luxembourg, 16 July 2020, found at http://curia.europa.eu/juris/document/document.jsf?docid=228677&pageIndex=1&occ=first&part=1&text=&dir=&doclang=EN&mode=req&cid=15482677 visitation date 5/8/2020

[74] Ibid, paragraphs 178-185

[75] Ibid, paragraphs 190-197

[76] Ibid, paragraphs 122-149, ruling 4

Alternatives to limit the total disruption of the trade relationships between the EU and the U.S. are Standard Contract Clauses (SCC) and Binding Corporate Rules (BCR). Although they were initially made to govern simple transfers from point A to point B, they weren't fully equipped to handle the intrinsic mechanisms involved in today's transfers which could be complicated and time-consuming to fully implement. As a result, more demands and obligations were placed upon these companies and organizations to guarantee the optimal functionality of the SCC and BCRs through conducting due diligence and suitable modifications before blindly relying on them [77].

As portrayed through the aforementioned information, international efforts in finding an adequate and equally representative system of cross-border data transfer that satisfies every country's vision and priority have proven strenuous. Reasons for such incompatibilities stem from the fundamental and unchanging values and beliefs that each country or region was built upon. While the EU holds the right to privacy and data protection as the number one priority, the U.S. puts the general economic order through free trade and open borders as its primary concern. At this time, the equal coexistence and preservation of both values without risking one in favor of the other is hard to envision, especially since politics has become the main driver of these policies. It remains to be seen what the third version of the co-regulatory agreements between the EU and the U.S. will be like.

[77] Katherine Noyes, Deloitte, Privacy Shield is Dead. Now What? Article, published in The Wall Street Journal, September 11, 2020, found at https://deloitte.wsj.com/riskandcompliance/2020/09/11/privacy-shield-is-dead-now-what/ visitation date 15/10/2020

SUB-CHAPTER 2: The GDPR's Enforcement Mechanisms and Territorial Scope

The GDPR is considered to be a borderless regulation that aims to regulate a borderless phenomenon. For this reason, the study of the Regulation's implementation and enforcement mechanisms should be approached based on a multi-layered structure composed of a set of adjoining rights and obligations applied nationally and internationally. Thus, (Section 1) will be a demonstration of the rights and obligations of data controllers and the role of the DPA as enforcers of the GDPR. Additionally, it will cover the foundation of establishing sanctions and remedies. Moreover, it will present an overview of the cross-border data transfer mechanisms. Meanwhile, (Section 2) will analyze the territorial scope of the GDPR through a theoretical and practical demonstration.

SECTION 1: National and International Enforcement Mechanisms

This Section will cover the basic principles of the national and international enforcement mechanisms applied by the GDPR through the duties of a data controller, the role of the data protection authorities, the method of applying sanctions and remedies, cross-border data transfer, and some noteworthy practical examples.

A- The Duties of a Data Controller

Generally, a controller is an entity that either alone or jointly with others determines the means(how) and purposes(why) in which personal data are being processed[78]. They are responsible for guaranteeing that the processing of data is done in accordance with the GDPR requirements through implementing necessary technical and organizational protocols under accountability standards that require them to illustrate their compliance with the Data Protection Principles[79]. The compliance warranty also extends to overseeing and implementing safeguards in the planning or pre-initiation phase of any service or device used in data processing[80]. Additionally, a controller based outside the EU is tasked with appointing a representative in one

[78] General Data Protection Regulation, OP. Cit. supra note 2, Article 4(7)
[79] Ibid, Recitals 74,85; Articles 24, 5(2)
[80] Ibid, Rec.78; Art.25

of the Member States in cases where the controller offers goods, services, or keeps track of individuals in the EU. The appointment of a representative isn't necessary for minute-level data processing which doesn't include sensitive personal data. The appointment and work of representatives should be mandated by the controller or processor, and enforcement actions may be brought on representatives by the DPA for the failure of compliance from the controller[81]. Moreover, the appointment of data processors by a controller is permitted under the assurance of complying with the GDPR. An appointment must be done in a legally binding written form that covers issues of processing confidentiality, providing aid and information to the controller in showing compliance, implementation, and attaining DPA approvals, abiding by the controller's instructions which also include the appointment of a sub-processor[82]. Furthermore, a controller either alone or with his representative must keep records of their processing activities which are provided upon request to the DPAs[83]. Controllers must cooperate with the DPA[84], and report data breaches that are likely to cause harm to data subjects immediately or within a maximum of 72 hours of being aware of it, and a record of breaches should be kept[85]. Finally, notifying data subjects without delay of a breach is required from controllers so that data subjects could be aware and take protective measures to try to minimize their losses (changing passwords, replacing credit cards, extracting or withdrawing money or information, etc.,) but exceptions apply if the risk is insignificant or the data controller took protective measures to protect the data, or where notification demands are disproportionate which then requires a public notice announcement of the breach[86]. Security protocols constitute the basis of the GDPR, where controllers should guarantee protection through implementing safety measures such as personal data encryption, conducting regular reviews and tests of their security systems, initiating backup programs[87].

It is noteworthy to mention that in cases where there are joint controllers, each controller is fully liable to the data subject pursuant to the GDPR. This means that the data subject can bring a claim against any joint controller(s) for a data breach of his/her information. After paying full

[81] Ibid, Rec 80; Art. 4(17), 27
[82] Ibid, Rec. 81; Art. 28(1)-(3)
[83] Ibid, Rec. 82,89; Art. 30
[84] Ibid, Rec. 82; Art. 31
[85] Ibid, Rec. 73, 85-88; Art. 33
[86] Ibid, Rec. 73, 86-88; Art. 34
[87] Ibid, Rec. 83; Art. 32

compensation the designated controller(s) can recover damages from other controllers who were also liable and involved in the processing process. An exception applies if the controller isn't in any direct or indirect way responsible for the damage. As a result, joint controllers will try to protect themselves through contractual indemnities from one to another before engaging in joint processing[88].

B- Data Protection Authorities (DPAs)

DPAs are independent[89] and transparent authoritative bodies responsible for overseeing, enforcing, investigating, and bringing legal proceedings, if necessary, against those who breach. They also guide the implementation of data protection laws at the national level[90]. Member states are required to appoint single or multiple DPAs. They are tasked with, but not limited to, monitoring and enforcing the GDPR, promoting awareness related to risks, safeguard measures, and rights that accompany personal data processing, advising national and governmental institutions on the application of the GDPR, listening to claims brought by data subjects or representatives and inform them about the results of such claims, permitting model clauses and BCRs, establishing conditions for impact assessments and promoting the creation of codes of conduct, reviewing certifications, logging sanctions and enforcement actions[91], filing public annual activity reports[92], and fulfilling any required task related to protecting personal data.

Different Member State DPAs at a national level should coordinate[93], cooperate[94], and form consistency mechanisms[95] to attain the best possible result from enforcement and implementation of the data protection laws. For this reason, the EDPB is formed as a body of DPA representatives from each Member state, that provides guidance and has an active role in executing the EU data protection laws. Different DPAs could carry out joint enforcement operations and mutually aid each other when dealing with violations.

---

[88] Ibid, Rec.79; Art.27
[89] Ibid, Rec.117,118,121; Art.52
[90] Ibid, Rec.117, 129, Art.51, 58
[91] Ibid, Rec.122,123; Art.55,57
[92] Ibid, Art.59
[93] Ibid, Art.51(3), 69-76
[94] Ibid, Rec.133,134; Art.61-62
[95] Ibid, Rec.135-138; Art.4(23), 56, 63-67

These issues are directly related and important to the success of the "One Stop Shop" concept. The issue of one-stops hop is raised in predicaments where several DPAs are tasked with regulating the same activity concluded by the same organization in different member states. As a result, the notion of a one-stop shop intends to formulate a unified decision-making process in which a designated DPA takes the lead in regulating and overseeing compliance standards. This DPA is chosen based on the place where the controller has his main establishment at (main processing decisions are taken) and this is an objective condition that varies from case to case since the designation of the main establishment is directly related to the processing activities related to the lawsuit and not the main establishment of a company as labeled on paper. Consequently, the primary selected DPA has the power to regulate or control that controller across every member state even in cross-border data transfers[96]. This is shown in the previously explained *Schrems v. Facebook* case where the designated DPA was that of Ireland since Facebook's main establishment and controlling activities in Europe is in Ireland. Additionally, the issues of the one-stop shop and main establishment predicaments will be addressed in cases that involve France's DPAs.

C- Sanctions and Remedies

As established, DPAs are tasked with enforcing the GDPR. So, deciding on sanctions and remedies is exclusively part of their job description. Accordingly, data subjects are given the right to file complaints to the related DPA based on jurisdiction limitations such as where they live, work, established or where the violation occurred concerning the processing of their data, except for the one-stop shop condition that could affect the designation of the lead DPA[97]. Moreover, data subjects have a right to judicial remedy against unlawful processing of their data by controllers or processors or due to a decision taken by the DPA that concerns them, or from the negligence of the designated authorities to respond to or deal with complaints within 3 months[98]. Additionally, determining the venue for proceedings is a demanding task since processing activities might occur in a member state and affects a data subject in another member

[96] Ibid, Rec.124-128; Art.55-56; WP29 Lead DPA Guidelines found at https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp244_rev01_enpdf.pdf visitation date 25,6,2020
[97] Ibid, Rec.141; Art.77
[98] Ibid, Rec.143; Art.78,79

state. Under the GDPR venue designation is split into two: Proceedings against DPAs or public authorities take place in the member state where the DPA is established, and proceedings against a controller or a processor fall under the jurisdiction of the member state where the controller or the processor has their establishment or the member state where the data subject resides (except for of the case where the controller or processor is a DPA or public authority)[99]. This specific venue designation protocol could negatively reflect on organizations when legal proceedings occur in an unfamiliar jurisdiction. Furthermore, data protection legal proceedings are subject to suspension which will stop parallel court proceedings from taking effect. This happens when multiple complaints on the same subject are filed in multiple member states and multiple courts initiate in exploring these claims[100]. Moreover, data subjects have a right to be compensated for harm due to unlawful processing of their data from the controller or processor. The same liability principles apply as mentioned in the controller's obligations (including joint liability conditions[101]) and the processor's legal duties[102]. Exemption from such liabilities occurs when controllers or processors can prove that they are not responsible for the processing that caused the harm, but exemptions as a result of harm caused by a force majeure are not addressed[103].

Finally, DPAs should issue sanctions and administrative fines in a proportional, effective, and dissuasive manner. Administrative fines may be introduced by the DPA and imposed by national courts in the event of the absence of such fines by a member state's legal system[104]. These administrative fines are bound by a ceiling of "the greater of €20 million or 4% of an undertaking's worldwide turnover for the preceding financial year" [105]. Due regards must be given by the DPA when considering the value of fines to be issued to ensure consistent application and proportionality of the EU law. Considerations for fines include: nature, gravity, and duration of the infringement; the number of affected data subjects and the degree of harm inflicted; the type of infringement- whether intentionally done or as a result of negligence-; past controller or processor infringements-if found-; the degree of assistance from the DPA; if the

[99] Ibid, Rec.143; Art.78(3), 79(2)
[100] Ibid, Rec.144; Art.81
[101] Ibid, Rec.79, 146; Art.26(3), 82(3)-(5)
[102] Ibid, Rec.146-147; Art.82(1)-(2), (4)
[103] Ibid, Art.82(3)
[104] Ibid, Rec.150,152; Art. 83
[105] Ibid, Art. 83(5)-(6)

violation was self-conveyed by the controller or processor; and any other significant factors[106]. Also, additional penalties and criminal sanctions are applicable by member states where administrative fines aren't applicable[107].

D-Cross-Border Data Transfer Regulations

The creation of a "virtual border control" by the EU came as a result of the speed and overwhelming amount of data being transferred across borders with a seemingly minute fee. Consequently, to preserve the forcefulness of its regulations, the EU -through the Data Protection Directive (95/46/EC)- addressed several issues concerning cross-border data transfer. The enactment of the General Data Protection Regulation (GDPR) saw the preservation of some principles, while others were either positively or negatively modified. Accordingly, they had an impact on states, companies, and organizations both legally and economically. Additionally, due to the time gap between the DPD and the GDPR during which a massive change in technologies used and cross-border commerce and e-commerce occurred, new concepts were addressed by the GDPR that were previously unforeseen in the 1990s.

There are general prohibitions on cross-border data transfers where a data subject from the EU is involved. These prohibitions can be lifted if certain requirements are met[108]. First of all, transfers are validated based on adequacy decisions given by the European Commission to third countries. These decisions are based on a study of countries' data protection systems. If third countries offer suitable protection on par with the GDRP then they are deemed as adequate countries for conducting transfers with[109]. These decisions are up for time-based reviews under certain conditions[110]. Second of all, cross-border data transfer is viable through agreements conducted by public authorities in the EU and in the third country where both authorities

[106] Ibid, Art.83(2)
[107] Ibid, Rec.149, 152; Art.84
[108] Ibid, Recitals 101-116; Art. 44,45
[109] Ibid, Rec. 103-107; Art. 44,45 - NOTE: Adequate Jurisdictions recognized by the European Commission are: Andorra, Argentina, Canada (for specific organizations subject to Canada's PIPEDA law), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay, while discussions on adequacy are ongoing with South Korea. See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,are%20ongoing%20with%20South%20Korea visitation date 9/6/2020
[110] Ibid, Rec. 106-107; Art. 45(3)-(5), 93(2)-(3)

guarantee compliance with the GDPR requirements[111]. Third of all, cross-border data transfer is viable through Binding Corporate Rules (BCRs). BCRs are authorized by the appropriate DPA and could include members of a corporate group found in third countries. Compliance of BCRs with the requirements of the GDPR exempts them from further authorization from the DPA[112]. Fourth of all, transfers are allowed based on Model Clauses or Standard Contract Clauses (SCCs) that are validated by the Commission[113]. Another form of SCCs adopted by one or several DPAs is the DPA clauses which also allow for cross-border transfers in conformity with the GDPR[114]. Fifthly, codes of conduct, coupled with binding and executable commitments in ensuring appropriate safeguards can be used to permit cross-border data transfer under the GDPR[115]. Sixth of all, transfers can be accredited via attaining certifications[116] or adding Ad-Hoc clauses[117] that show consistency in transfers and GDPR compliance. Last but not least, third country court judgments can permit cross-border data transfer, only if this transfer is covered by a suitable international agreement[118].

In turn, certain derogations may apply that allow for the transfer of data without having fulfilled the aforementioned conditions. These specific situations are: explicit consent by data subjects after being aware of the risks[119], contracts between a data subject and a controller where international data transfer is needed for performing and implementing purposes of the contract, contracts that serve the data subject's interest (e.g., parents buying on behalf of their child) in this case cross-border legality is viable on the grounds of the conclusion or performance necessitated by the contract, public interest -may also be considered as a basis for cross-border data transfer under the GDPR- if these interests are recognized by the EU or in the law a member state where the controller is subjected to, legal claims could also warrant a lawful international transfer of data when it essential legal proceedings, claims or obtaining legal guidance. Additionally, cross-border data transfers are justifiable and accepted when they are needed in

[111] Ibid, Rec. 108, Art. 46(2)(a), (3)(b)
[112] Ibid, Rec. 108, 110; Art. 4(20), 46(2)(b); WP256, WP257
[113] Ibid, Rec. 81, 108-109; Art. 28(6)-(8), 46(2)(c), 57(1)(j), (r), 93(2)
[114] Ibid, Rec. 108-109; Art. 46(2)(c), 57(1)(j), (r), 64(1)(d), 93(2)
[115] Ibid, Rec. 108; Art. 40,41, 46(2)(e)
[116] Ibid, Rec.108, Art.42, 43, 46(2)(f)
[117] Ibid, Rec. 108; Art. 46(3)(a), (4), 63
[118] Ibid, Rec. 115; Art. 48
[119] Ibid, Rec.111; Art.49(1)(a), (3)

protecting the vital interests of the data subject or his guardians when he isn't able to physically or legally provide consent. Finally, an international transfer may occur if the transferred data are obtained from a public register[120]. In a different context, transfers are permitted based on the compelling legitimate interest of the data controller which isn't overridden by those of the data subjects. The controllers are tasked with weighing the legitimate interest perceived from processing against the privacy rights of the data subjects. When the former prevails, processing could be done without obtaining consent but affected consumers are given notice to opt-out rather than opting in to obtain consent. Meanwhile, controllers will still be held liable for any misuse[121]. The issue of legitimate interests is a subject of an ongoing debate due to its broad interpretations and vagueness.

E- Some Conflicts in the Practical Application of the Cross-border Data Transfer Stipulations

First of all, several arguments question the practical application of the SCCs. One of those arguments is that the SCCs are outdated since they were last modified in 2010 which is 8 years before the adoption and implementation of the GDPR. Thus, they fail to acknowledge the additional rights and obligations placed on data processors and data controllers established in the GDPR. For example, the insertion of SCCs in contracts between an EU data controller and a third country data processor (Controller to Processor C2P SCCs). The GDPR added to the obligations of these processors, that aren't mentioned in the current C2P SCCs[122]. Another criticism of the SCCs is that although they must be approved by the European Commission before adoption, they are initially adopted individually by each National Supervisory Authority[123]. This could result in different SCCs in different Member States that could offer different methods of protection. Hence, working against the desired goal of the EU to harmonize data protection across Europe.

---

[120] Ibid, Art. 49

[121] Ibid, Rec. 113, Art. 49(1), (3), (6)

[122] Marko Popovic, of (BDK Advokati), Standard contractual clauses challenged by the GDPR and scrutinized by CJEU, Article, published February 9, 2018, found at https://www.lexology.com/library/detail.aspx?g=d4a4a515-4868-4445-8b1c-0d358feab8fe visitation date 6/4/2020

[123] GDPR, OP. Cit. supra note 2, Articles 46(2)(c); 93(2)

Second of all regarding consent, it remains unclear as to how much information concerning the transfer should be given to the data subject by the transferring party[124]. Additionally, vagueness surrounds the issue of whether transferring parties should give out the specified risks relating to cross-border transfers to particular third countries, or whether a general disclaimer would suffice[125]. Moreover, according to authors Paul Schwartz and Karl- Nikolaus Peifer, the EU legislators in issues of consent preferred to follow a collective approach to consent and contract doctrine. However, they favor the concept of information privacy inalienability[126]. According to Susan Rose-Ackerman, inalienability is defined as "any restriction on the transferability, ownership, or use of an entitlement"[127]. This idea backs the notion that individuals might not be as free as they would like to believe concerning their data, since there are some cases that an individual can't consent to[128]. Consequently, information privacy inalienability limits an individual's ability to freely control his/her data, including situations via consent or contract. Thus, creating areas of non-contract and non-consent[129]. For example, the European data protection laws have cases where data subjects can't waive or trade some rights. Furthermore, Albrecht and Jotzo noted that "a data subject cannot through consent 'sell' fundamental rights protected by the Charter, including the fundamental interest in privacy and data protection"[130]. Thus, it seems counter-intuitive to allow data subjects to consent on data transfers to third countries that may neither provide minimal protection nor that don't have protection standards at all. Although there is an information presentation obligation, that doesn't mean that data subjects will actually read and understand several pages of terms and conditions that are complicated and

[124] Paul Voigt, Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer International Publishing, 2017, page 118
[125] Ibid, page 119
[126] Paul M. Schwartz, Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, Publication in the Georgetown Law Journal, Vol 106:115, 2017, pp. 115-179, page used 139, found at https://escholarship.org/content/qt1ws1r1cz/qt1ws1r1cz_noSplash_816c6e2b4eaaaec14b0a03ecedd4031b.pdf?t=p68tx6 visitation date 6/4/2020
[127] Susan Rose-Ackerman, Inalienability and the Theory of Property Rights, Publication in Columbia Law Review Vol. 85, No.5, June 1985, pp. 931-969, page used 931, found at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1592&context=fss_papers visitation date 20/5/2021
[128] Paul M. Schwartz, Privacy Inalienability and the Regulation of Spyware, Publication in Berkeley Technology Law Journal, Vol. 20, 2005, pp. 1269-1282; See also Paul M. Schwartz, Property, Privacy, and Personal Data, Publication in Harvard Law Review, Vol. 117 Rev. 2055, 2003-2004, pp. 2056-2128, page used 2095
[129] Ibid
[130] Jan Philipp Albrecht, Florian Jotzo, Das Neue Datenschutzrecht Der EU "The EU's New Data Protection Law" published by Nomos, Germany,126-29 (2017), page 72, could be also found at Schwartz (Paul M.), Peifer (Karl-Nikolaus), Transatlantic Data Privacy Law, OP. Cit. supra note 126, page 140

smartly written in ways that would mislead them[131]. So, it is believed that adjoining privacy rights and data protection with fundamental rights in the Charter was done to avoid data subjects waiving these rights to offer them protection. However, this protection could disappear if transfers to third countries without protection could be done through consent alone.

SECTION 2: The Territorial Scope of the GDPR

This Section will provide a combination of a theoretical and a practical application of the aforementioned national and international obligations under the GDPR. The study of practical implementation of the GDPR's scope of application will be based on the analysis and interpretation of its territorial and extraterritorial scope established by Article 3.

A- The GDPR's Scope of Application

Article 3 of the GDPR defines the territorial scope of the Regulation that is needed to cope with the borderless nature of the internet. Accordingly, the terms used in Article 3 aim to maximize the protection of data subjects by validating the applicability of the GDPR outside the Member States of the European Union. Two main principles justify the extraterritorial reach of the GDPR which are: the establishment principle and the lex loci solutionis rule (place of performance).

a) The establishment principle

According to Article 3(1) of the GDPR, the rules of this regulation apply to "processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not"[132]. Under this principle, the applicability of the GDPR depends on whether the establishment of the controller is located in the European Union; not where the actual processing of data is happening[133]. Accordingly, entities that aren't located in the EU, but engage in processing activities through subsidiaries or international branches located within the EU must abide by the GDPR. Thus,

[131] Schwartz (Paul M.), Peifer (Karl- Nikolaus), Transatlantic Data Privacy Law, OP. Cit. supra note 126, page 171
[132] GDPR, OP. Cit. supra note 2, Article 3(1)
[133] Voigt (Paul), Von dem Bussche (Axel), OP. Cit. supra note 124, page 22

even if subsidiaries don't carry out the specified processing activities, but are located in the territory of one or more member states; are deemed as establishments within the context of the GDPR, the main branch or headquarters of the establishment will have to comply with the GDPR even if it is outside the EU if the processing is considered to be within the "context of activities" of the subsidiaries.

Therefore, the applicability of Article 3(1) of the GDPR is based on the data controller or processor having an "Establishment" in the EU. Article 3(1) doesn't define what an establishment is, but Recital 22 of the GDPR sheds some light on what considerations must be taken into account when determining an establishment. It states that an establishment must be understood as "the effective and real exercise of activity through stable arrangements"[134]. Additionally, it diminishes the importance of the legal form of the entity located in the EU, whether it's a branch or a subsidiary of a mother company. Moreover, since the interpretation of what an establishment is in both the GDPR and the DPD are identical, a case law presided over by the ECJ could be of use. In the case of *Google Spain v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, the ECJ considered that "establishment" can't be given a restrictive definition[135]. Another example is the 2015 case of *Weltimmo sro v. Nemzeti adatvedelmi es informacriowasbadsag hatosag*, the court referred to Recital 22 to define an establishment. The court held that "stable arrangement" should be put in the context of the economic activities of the entity and services offered[136]. This means that determining if an entity is an establishment is case-relative, and the term "stable arrangement" should be taken into account when determining the scope of activities. In other words, if a single person is present in the EU and provides services within a stable manner, it would be sufficient to deem him as having an establishment in the EU. Thus, subjecting him to the GDPR. Hence, the ECJ in the *Weltimmo Case* disregarded the traditional notion of entities having only one establishment

[134] GDPR, OP. Cit. supra note 2, Recital 22

[135] CJEU (Grand Chamber), Judgment of the Court in Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, May 13, 2014, paragraph 53, found at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62012CJ0131 visitation date 2/4/2020

[136] CJEU (Third Chamber), Judgment of the Court in Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, October 1, 2015, paragraphs 28-31 and 41, found at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0230 visitation date 4/7/2021

located in the state where it is formally registered. Nonetheless, the place of registration is still important in indicating its location, but not entirely sufficient or decisive.

Another aspect of Article 3(1) is that it also mentions that processing needs to take place "in the context of activities" of the establishment located in the EU. Accordingly, establishments must be involved in the activities which result in the processing of the data. For example, the ECJ in the aforementioned Google Spain case based its decision to consider the entity as an establishment in the EU on the economic activity that linked the establishment to data processing. It considered that the activity of running a search engine was related to the activity of selling advertising space which turned out as the main activity of the subsidiary in Spain. The ECJ reasoned that the search engine was making profits because of the selling of advertising space, and the success of the search engine (data processing) was necessary for the activity of selling the advertising space (activity of Google Spain)[137]. Thus, merging the idea of data processing and the activities of the establishment based on an economic link between them.

Such cases show the flexibility in which the broad statements in the GDPR can be defined and interpreted in accordance with the facts of each case. Thus, the determination of whether an entity is an establishment or not under these laws is open-ended and complex, which can be given several interpretations per what courts deem befitting of the case. Hence, this results in unexpected court findings and somewhat different outcomes.

b) Lex Loci Solutionis

According to Article 3(2) of the GDPR, the regulation applies if the processing of personal data of data subjects is carried out by a controller or a processor not based in the EU if processing activities are related to "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 the monitoring of their behavior as far as their behavior takes place within the Union"[138]. Thus, the applicability of the GDPR is valid even if the controller and processer aren't located in a Member State. Hence, determining the applicable law is based on the place of the relevant and necessary contractual performance being offered or where the monitoring of personal behavior of data subjects is

[137] Google Spain case, C-131/12, OP. Cit. supra note 135, paragraphs 52 and 56
[138] GDPR, OP. Cit. supra note 2, Article 3(2)

happening (Lex Loci Solutionis Principle)[139]. Accordingly, the extraterritorial jurisdiction of the GDPR can be achieved through two methods:

1- Offering of goods and services to data subjects in the EU

Through these activities, the GDPR is trying to cope with the nature of the internet and the borderless world it created. International entities can offer goods and services over the internet (even for free) to customers without physical interaction or presence. For this reason, the GDPR wanted to limit the unrestricted accessibility and activity of non-EU companies targeting EU consumers, that would want to avoid EU regulations by not being present in the EU. Accordingly, Recital 23 of the GDPR provides examples of how non-EU companies target EU customers in a way that makes them liable under the GDPR. For example, using language which is spoken in EU states, accepting EU currencies (especially Euros), offering delivery to EU states, or the specific mentioning of customers from Europe. Therefore, it is easy for an entity outside the EU to be considered as "offering goods and services" to EU customers, regardless of whether a positive action by them is required[140].

2- The monitoring of data subjects' behavior in the EU

Monitoring is a broad term that can encompass tracking techniques or profiling whether normal or automated. Profiling is done by almost all big data companies and social media platforms. They use data to enhance the users' online experience and tailor their accounts according to their interests. It is a data-gathering method used in predicting users' preferences, behaviors, or attitudes[141]. This way is used to open up such platforms for advertisers to promote certain products and ideas that drive individuals consciously or subconsciously into adopting them. Although these techniques could enhance user experience, when abused they could result in dangerous outcomes. For example, the Cambridge Analytica scandal in 2018 where Facebook users' data was processed without their consent to target political advertising and influence

[139] Voigt (Paul), Von dem Bussche (Axel), OP. Cit. supra note 124, page 26
[140] GDPR, OP. Cit. supra note 2, Recital 23
[141] Ibid, Recital 24

elections[142]. Therefore, the GDPR aims through this provision to extend its application to non-EU entities that engage in these activities and protect EU data subjects' data.

In conclusion, the theoretical adoption and application of the GDPRs extraterritorial jurisdiction is a step forward in terms of universally setting a standard of protection, that can reach a great number of people and entities all over the world. Additionally, it directly and indirectly appealed to data subjects all over the world which resulted in a significant increase in awareness and a change in attitude concerning data protection and their privacy rights. However, until now, the practical application of the GDPR's extraterritorial reach is far from ideal. Unilaterally deciding upon rules that govern the borderless and complex nature of the internet and its byproducts by independently constructing a borderless and complex set of regulations isn't a viable solution. Additionally, following a system of inclusion and exclusion regarding transfers based on whether "a country is either adequate or not" and adding limited derogations or depending on certain clauses, doesn't conform with the interconnected nature of how societies function. In other words, imposing a standard of laws that is essentially connected to every transaction that could be possibly made through the technologies of today's world is impossible. For this reason, through the examples of the Schrems cases and those yet to come, we will notice a judicial and extra-judicial discombobulation in handling cases and delivering justice. Also, the discussion of some loopholes in the extra-territorial function of the GDPR, especially through the conflicts it manifested with the U.S., will serve as an example of the difficulties and sensitivity of trying to implement a solely established regulation on two entities that share different beliefs, and base the entirety of their systems on those beliefs. Finally, this can be attributed to jurisdictional conflicts, overlapping or entirely different regulations, contradicting obligations of entities tasked with overseeing implementation, and the involvement of several international actors. Eventually, it will harm those whose rights have been violated, draining their resources, consuming their time, and reflecting negatively on the integrity and grit of the judicial and extra-judicial systems.

[142] Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, Article, published in the New York Times, April 4, 2018, found at https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html visitation date 4/4/2021

CHAPTER 2: The GDPR's Impact on Judicial Decisions and Extra-Judicial Functions

The nascent data protection laws and privacy regulations elevated the status of a person's digital protection and privacy to an almost infrangible right. It became clear in the previous part, that the borderless nature and rigor of the GDPR changed the dynamics of how countries, states, public and private entities, companies, and individuals; operate, conduct their day-to-day transactions, and manage the data they acquire. As also touched upon, these events paved the way for new obligations, adequacy measures, intricate and costly procedures, which had to be properly adhered to, in order to protect peoples' data and privacy. Thus, the laws and principles which were in place had to accommodate the new requirements of the GDPR and other data protection regulations. Although these novel standards are necessary for this digitally propelled age, some deemed them as arduous nuisances. The numerous sacrifices and adjustments that needed to happen to adapt to these regulations caught everyone off-guard, which caused several inter and intra-state collisions. These predicaments are clearly perceived through the procedural and practical development in judicial decisions (Sub-Chapter 1). Moreover, data protection and privacy regulations also became enmeshed with the fabrics of extra-judicial functions. ADR, especially arbitration is a data-based institution that has both- national and international- reach. Accordingly, (Sub-Chapter 2) will address the influence of modern digitalization on arbitration processes through its combination with the GDPR.

SUB-CHAPTER 1: The Implementation and Defects of a Borderless Regulation

It has become clear that the EU aims to harmonize data protection laws throughout Europe and extend that protection extraterritorially to every part of the world. However, the extraterritorial application of these Regulations is a double-edged sword, meaning that the unilateral decision taken by the EU to internationally apply its regulations in a field governed by a borderless nature (internet/ technology) is problematic. For this reason, (Section 1) will cover how the extra-territorial reach and application of the GDPR could be justified under the principles of international law. Whereas, (Section 2) will shed light on the shortcomings of the GDPR through its borderless nature.

SECTION 1: The Practical Application of the GDPR on Judicial Cases

This section will be dedicated to addressing the procedural issues of applying the GDPR extra-territorially on judicial disputes. Moreover, through multiple case analyses handled by France's DPAs, this section will cover the role of local data protection authorities (DPA) in France (CNIL) and the extent of their powers beyond European jurisdictions; in addition to the degree of enforceability of European judgments on other countries.

Sub-Section 1: Procedural Issues Regarding the Application of the GDPR's Scope

A- Struggles with International Law

The application of the GDPR through Article 3(2) which promotes the idea of Lex Loci Solutions, implies that the applicable law is designated by the location of where contractual performances are being offered. This means that the place where the establishment of the controller or processor is found isn't the deciding factor. Additionally, it has been established that the "offering goods and services" and the "monitoring of data subjects" have been broadly interpreted by courts[143]. Thus, using Article 3(2) and Recital 23 of the GDPR and applying it to a situation presented by authors De Hert and Michal Czerniawski, in which an EU Data Subject

[143] Alexander Kloth, One Law to rule them all, On the extraterritorial applicability of the new EU General Data Protection Regulation, Article, published on Volkerrechtsblog, 5/2/2018, found at https://voelkerrechtsblog.org/one-law-to-rule-them-all/ visitation date 4/4/2021

books a trip to the U.S. using a US travel agency's website that offers the option of choosing a language used in Europe (i.e., French, Spanish, English) and to pay in Euros[144]. This would suffice as "selling goods and services" to EU Data Subjects. Therefore, the GDPR is applicable[145]. Although this example has the elements prescribed by the GDPR to enforce its regulations, it could be debated that the performance of the main elements of the contractual clauses (payment and other services) are based and will happen in the U.S.[146] Hence, causing a conflict of laws between the EU and U.S. laws, that regulate data protection differently. As previously discussed, and exemplified in the Schrems cases, the U.S. intelligence services could ask for or directly access the data of the U.S. travel agency which includes information about the EU data subject[147]. This act is not permitted under the EU law, but the American agency is more likely to conform with the U.S. law and will be obliged to hand over their data rather than refraining, in favor of the EU law. Hence, the enforceability of the GDPR on entities not based in countries that have different data protection regulations is of concern.

This is also the case in the application of Article 3(2) (b) and Recital 24 which covers the tracking and monitoring data subjects' behavior using profiling or other data processing techniques. This Article applies to establishments that are not based in the EU but target EU data subjects. Understandably, this stipulation in enforcing the GDPR has to do with limiting the exploitation of personal information from big data companies using "cookies" such as Google and Facebook as described in detail in the following Section. However, since almost all countries have entities that are based online and use "cookies", enforcement of such clauses is difficult when the entity doesn't have an establishment or subsidiary based in the EU[148]. The alternative would be to block the websites that don't conform to this regulation.

[144] Paul de Hert, Michal Czerniawski, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, Article, published in International Data Privacy Law, Volume 6, Issue 3, August 16, pp. 230-243, page used 230, found at https://academic.oup.com/idpl/article/6/3/230/2447252?login=true visitation date 15/4/2021

[145] Kloth (Alexander), OP. Cit. supra note 143

[146] Ibid

[147] Ibid

[148] Ibid

B-Issues Concerning the Jurisdiction of European DPAs and EU Courts

The application of the GDPR in countries outside Europe requires its establishment as an applicable international instrument in these countries, and the involvement of National Courts in Europe, the ECJ, and the European Data Protection Authority that relate to the case. However, it is a difficult task to apply foreign laws in other countries especially with the jurisdictional principles established in international law. For example, the territorial principle stipulates that a state has jurisdiction over events that happen in its territory[149]. Another example is the effects doctrine, which is a basis for jurisdiction over acts of foreign nationals committed abroad but has consequences in the original country (extension of the objective territorial principle)[150]. Essentially, a justified jurisdictional exercise over a case using any principle should require a sufficient and impactful connection between the events of a case and the state that seeks to exercise its jurisdiction[151]. Consequently, it might be difficult to assign jurisdictional authority to EU Courts and DPAs per the stipulations of the GDPR concerning online activities that take place in counties outside Europe having different data protection regulations and are keen on applying the territorial jurisdiction principle. Additionally, the fact that the GDPR has an overreaching extra-territorial application that is justified based on minute details, occurrences, or people, will surely cause conflicts of jurisdiction between the EU and other countries.

C- Enforcement Issues Concerning Fines

The GDPR has provided DPAs with the power to enforce massive fines (i.e., up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year; and up to €20 million or up to 4% of annual worldwide turnover for entities that breach the GDPR concerning cross-border data transfers)[152]. However, these fines are used in a punitive manner as the last resort for non-compliance, for the goal of the GDPR is to ensure compliance through guidance and warnings to balance between EU citizens' rights and secure business opportunities in Europe

[149] Hannah L. Buxbaum, Territory, Territoriality, and the Resolution of Jurisdictional Conflict, Articles by Maurer Faculty, published in The American Journal of Comparative Law, Volume 57, 2009, pp. 631-675, page used 636, found at https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1132&context=facpub visitation date 5/4/2021

[150] Ibid, pages 637-639; 667-669

[151] Restatement (Third) of Foreign Relations Law of the United States, 1988, Section 402 (1)(c); Section 403(1)

[152] GDPR, OP. Cit. supra note 2, Article 83(4),(5)

safely[153]. DPAs can issue and apply these fines with relative ease concerning establishments located in the EU. However, enforcing these fines on entities that aren't located in the EU and violate the GDPR based on Article 3(2) may prove to be difficult. These cases will need the cooperation and reliance of the EU on local authorities in third counties to follow through on the administration of fines. However, as shown, not all countries regulate or view data protection similarly to the EU. For example, the U.S. would only apply foreign judgments on cases when they pose no conflicts to Constitutional rights, rights protected by Federal or State laws, or any public policy considerations[154]. This is especially troublesome in cases where an entity i located in the U.S. and isn't part of the bilateral agreement on data protection between the EU and the U.S. Moreover, administering fines on entities in third countries that aren't directly linked to the EU is difficult, which undermines the true purpose of the GDPR. However, violating entities will surely face reputational repercussions which will affect their business and maybe ruin their future goals of expanding to other countries, especially to the EU.

After giving an insight into the extraterritorial reach of the GDPR about the processing of Data Subjects' data inside and outside the EU, with the practical conflicts that might encounter its application. It is important to study the mechanism and stipulation that allow for a legal data transfer to be carried out to countries outside the EU.

Sub-Section 2: France's Practical Implementation of the GDPR Through its DPA

A- A Case Triggered by Specific Complaints

A very recent and landmark case involving the French Data Protection Authority (CNIL) and Google which resulted in a fine worth €50 million could exemplify the enforcement mechanisms and capabilities of the European data protection regulations.

[153] Jan Philipp Albrecht, How the GDPR Will Change the World, Article, published in EDPL, 3/2016, pp. 287-289, found at https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf visitation date 5/4/2021
[154] US District Court for the District of Columbia, Vladimir Matusevitch v. Vladimir Ivanovich Telnikoff, Civ. A. No. 94-1151 RMU – 877 F. Supp.1 (1995) January 27, 1995; United States District Court, D. Delaware, Victoria del la Mata v. American Life Insurance Company, Civ. A. No. 90-173 MMS- 771 F.Supp. 1375 (1991), August 8, 1991, paragraphs 1375-1384

The CNIL went forward with an enforcement action against Google LLC. based on complaints filed by two non-profit associations called None of Your Business (NOYB) from Austria (founded by Max Schrems), and La Quadrature du Net (LQDN) from France, in May 2018[155]. The premise of this case revolves around Google's failure to comply with the transparency and notice requirements of the GDPR, and failure to acquire valid consent from users in the processing activities conducted by them through their Android operating system.

Deliberation of this case was done by the Restricted Committee on January 21, 2019. The following issues were addressed:

a) Procedural law issues: Competence of CNIL

Google built its primary argument on two facts. First, that its Ireland located establishment is considered as the "Main Establishment" and this case involves cross-border data processing and transfers, thus these procedures are not within France's CNIL's jurisdictional reach and should be referred to Data Protection Commission (DPC) in Ireland[156]. Second, it pointed at the lack of cooperation and consistency mechanisms from several Member State DPAs, given the cross-border nature of processing and the number of Android users affected. Additionally, due to the doubt created on designating the lead authority, Google asked for the case to be referred to the EDPB[157].

The Restricted Committee found that:

Firstly, regarding the "main establishment" claim, the Committee decided that Google Ireland Limited can't be considered as the main establishment, since under the objective criteria in determining the main establishment related to cases where multiple establishments are located in different Member States, Google Ireland wasn't awarded or given the decision-making power regarding the processing activities and setting the privacy policy of its mobile phones under the

[155] The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019, found on the official CNIL website: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc#:~:text=The%20fine%20imposed%20by%20the,limits%20provided%20by%20the%20GDPR. Visitation date: 17/10/2020

[156] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2017 pronouncing a financial sanction against GOOGLE LLC. paragraphs 23-25, found at https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf visitation date: 17/10/2020

[157] Ibid, paragraph 26

specified Android operating system. Additionally, Google Ireland wasn't designated in Google's "Privacy Policy" terms that it was Google's main establishment in the EU related to the processing activities addressed in this case. So, CNIL was considered the competent authority on grounds of the omittance of designating a main establishment which resulted in the absence of a lead authority[158].

Secondly, regarding the EDPB and the application of cooperation and consistency procedures. The Committee based its decision on the absence of a designated main establishment concerned with the proceeding at hand, and this issue creates uncertainty about the identification of a supervisory authority as a leading one. Thus, the one-stop shop mechanism doesn't apply to this case. Hence, there wasn't a need to refer this case to the EDPB. Also, the Committee noted that communications directly initiated by the CNIL with all supervisory authorities via the European information exchange system to determine a potential lead authority is a prerequisite of the one-stop shop protocol and constitutes as a fulfillment of the cooperation requirements of the GDPR. Moreover, it was established through the CNIL's activities with European authorities such as inquisitions, consultations, and frequent investigation and abidance by EDPB guidelines, that it had met the consistency and cooperation demands[159].

b) Privacy Violations

Based on investigations conducted, the CNIL's Restricted Committee came to observe two types of breaches of the GDPR.

1- Violations related to transparency and information requirements:

The Committee established that how information related to the company's privacy policies was structured made it hard for users to access and understand. Important information about processing purposes, storage periods, or types of data used for ads personalization was scattered across multiple documents which required a lot of time and effort to figure out, especially that relevant information is buried deep within a system of multiple steps and clicks[160]. For example, for the normal user to grasp the privacy protection mechanism related to advertising

[158] Ibid, paragraphs 28-41
[159] Ibid, paragraphs 49-55
[160] Ibid, paragraphs 97,98

personalization processing, he must read the general “Privacy Policy and Terms of Service” then click on “More options” followed by “Learn more” linking him to “Personalized advertising” which will be insufficient, because acquiring the full terms is done by going to “ Provide personalized services” section in the “Privacy Policy” document accessible through “Privacy policy and Terms of Services”, and the same applies to geolocation data processing[161].

Additionally, due to the nature of Google that is integrated into almost every field and with the interconnectedness between multiple processing technologies, especially those linked with Android account creating and its association with at least twenty other services (YouTube, Gmail, third party websites and applications), makes understanding the extent of the information that is being processed intrusive, unclear and incomprehensible[162].

2- Violations of the obligation to have a legal basis for ads personalization processing:

Google claimed to obtain clear and unambiguous consent as prescribed by the GDPR for such processing purposes[163]. The Committee established that the consent in question isn’t valid because it is immersed in several documents and doesn’t allow the user to fully acknowledge the extent of the ads-personalization processing operation. Furthermore, the attained consent isn’t specific nor unambiguous since upon creating the account, the user can alter and reconfigure the display of personalized ads by clicking on “more options” and the display of the ads-personalization consent is pre-ticked so the user should untick to show his disapproval[164]. Finally, consent is generally and vaguely imposed on users once they create an account by ticking boxes such as “I agree to the processing of my information as described above and further explained in the Privacy Policy”. Thus, by accepting, the user- through one undifferentiated motion[165]- gives his consent to every other service and processing operation provided by Google without being specifically asked to submit his consent to these processes[166].

On these Grounds, the Restricted Committee found that a violation of the privacy and data protection policies under the GDPR has been committed and the CNIL’s €50 million fine stands,

[161] Ibid, paragraphs 99,100
[162] Ibid, paragraphs 104-107; 109,110; 117; 121
[163] Ibid, paragraph 134-140
[164] Ibid, paragraph 145,146; 153
[165] Ibid, 159
[166] Ibid, paragraph 154,158,160

according to its €325 million turnover in 2017[167], the proportionality measures, grave implications, continuous nature of the infringement, Google's prominent position in the operating systems market and the huge number of people and millions of data worth of processing compromised[168].

On June 19, 2020, France's Highest Administrative Court ("Conseil d'Etat") upheld the decision of CNIL to impose a €50 million fine on Google LLC under the GDPR[169].

B-Cases Initiated *Sua Sponte* (on its own motion) by the CNIL

Contrary to the previous case where the CNIL followed up on specific complaints registered by companies for breaching data protection regulations, the following cases showcase the diverse powers of the CNIL and its independence in issuing fines and prosecuting violators.

In a timeframe of almost a year, from the end of 2019 till mid-2020, the CNIL went through several online investigations of google.fr and amazon.fr concerning cookie[170] policies, before initiating a full investigation into Google LLC, Google Ireland, and Amazon Europe Core. These investigations resulted in sanctions and fines totaling €135 million spread between Google LLC (€60 million) and Google Ireland (€40 million)[171], and Amazon Europe Core (€35 million)[172].

[167] Ibid, paragraphs 2, 189
[168] Ibid, paragraphs 176- 190
[169] The Council of State deciding on CR litigation, No. 430810, GOOGLE LLC COMPANY, Session of June 12, 2020, Reading of June 19, 2020, found at https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil visitation date 17/10/2020
[170] Definition of "Cookies": "Cookies are text files with small pieces of data- like a username and password- that are used to identify your computer as you use a computer network. Specific cookies known as HTTP cookies are used to identify specific users and improve your web browsing experience" … "When the cookie is exchanged between your computer and the network server, the server reads the ID and knows what information to specifically serve to you"… " HTTP cookies, or internet cookies, are built specifically for Internet web browsers to track, personalize, and save information about each user's session" – For more on "cookies" go to https://www.kaspersky.com/resource-center/definitions/cookies visitation date 4/10/2021
[171] Deliberation SAN-2020-012 of December 7, 2020, concerning the companies GOOGLE LLC and GOOGLE IRELAND LIMITED, paragraph 139, found at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706 visitation date 4/10/2021
[172] Deliberation SAN-2020-013 of December 7, 2020, concerning the company AMAZON EUROPE CORE, paragraph 125, found at https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635729 visitation date 4/10/2021

a) Procedural Law Issues: Competence and Jurisdictional Scope of the CNIL

To reach its decision the CNIL used Article 82 of the French Data Protection Law which transposes Article 5(3) of the ePrivacy Directive instead of the GDPR. By doing so the CNIL blocked any counterclaims in relation to its competence under the GDPR's one-stop shop structures. As explained, the one-stop shop principle stipulates that the designation of the lead investigative authority concerned with investigations and sanctions is determined by the location of the involved company's main establishment. Thus, both companies argued that under this principle the DPA of the EU Member States in which the two companies' main establishments are located (i.e., Ireland for Google and Luxembourg for Amazon) shall be responsible for this case. The same claim was also raised in the previously mentioned case. However, the CNIL's rebuttal was based on Recital 173 of the GDPR and the EDPB's opinion that confirmed that the GDPR shall only apply to the processing of personal data which is not subject to specific obligations set out in the ePrivacy Directive. Through this claim, the CNIL asserted its authority to control and sanction the use of cookies placed on devices owned by users located in France under the French Data Protection Act and the ePrivacy Directive. Therefore, the one-stop shop stipulation did not apply, since the decisions were not based on the GDPR. Additionally, since Google and Amazon had establishments in France, the CNIL's territorial competence can be justified[173].

b) Legality of the Decision

Article 82 of the French Data Protection Act applies and transposes Article 5(3) of ePrivacy Directive concerning the cookie rules -instead of the GDPR- stipulates that all non-essential cookies should be subject to clear and complete information presentation regarding the purposes of the cookies and how a user may block or refute their use. Additionally, prior consent of the user after the communication of such information is needed before actions are taken. The CNIL found in its decision that Google had violated three aspects of Art. 82. It failed to obtain consent, failed to provide the sufficient information needed, and didn't respect the right to offer objection to the use of certain cookies, for not all cookies were removed after user objection[174]. Whereas, Amazon violated Art. 82 in two aspects which were: lack of consent and insufficient

[173] Ibid, paragraphs 18-52; paragraphs 22-46 of Deliberation SAN- 2020-012, OP. Cit. supra note 171
[174] SAN- 2020-012, OP. Cit. supra note 171, paragraphs 67-109

information. The immediate drop of cookies upon a user's visit to the websites, before any presentation of relevant information to obtain a user's consent was of great importance to the CNIL in building a case around the breaching companies[175].

c) Administration of Fines

Both Google and Amazon opposed the fines issued by the CNIL. Google claimed that they were disproportionate and lacked formal guidelines for their calculation[176]. Whereas, Amazon based its claim on the fact that the fines exceed those that were issued by other authorities concerning breaching of the cookie rules, and that the CNIL failed to take into consideration the measures it had already taken, and that Amazon had not been a subject of prior investigations concerning such matters[177].

However, CNIL argued that it had discretionary powers to impose sanctions as it deems appropriate and within the confines of the French Data Protection Act (which is 2% of the worldwide revenues of the company). In addition to the fines, Google and Amazon were obliged to fix their practices and comply with the data protection regulations within three months of the decision, facing a penalty of €100,000 fine per day[178].

From what was demonstrated through the aforementioned cases, several conclusions can be reached. First of all, the CNIL and other data protection authorities are very keen on upholding and maintaining the principle of transparency and the ease with which users and data subjects can know how and when their personal data are being processed. Second, the preceding cases showed the capacity and the spectrum of power that data protection authorities enjoy. As demonstrated, the CNIL took the basic role of following up on a complaint and issuing suitable fines and took it upon itself to conduct online investigations through directly accessing these websites and testing their data protection measures, and determining whether they are adequate and on par with the GDPR and other data protection regulations. This action should become a trend among other DPAs since it could be beneficial in terms of preventing establishments from maneuvering around data protection regulations and acquiring the personal data of any data

[175] SAN- 2020-013, OP. Cit. supra note 172, paragraphs 77- 111
[176] SAN- 2020-012, OP. Cit. supra note 171, paragraphs 120,121
[177] SAN 2020-013, OP. Cit. supra note 172, paragraphs 114
[178] Ibid, paragraph 112; paragraph 138, 145 of SAN-2020-012, OP. Cit. supra note 171

subject who is unaware of such regulations, rather than waiting for data subjects to issue complaints. Additionally, their specialized knowledge in this field makes it easier for them to catch violators, instead of normal users filing wrongful claims that could cost companies time, reputational damage, and financial burdens through litigation. Finally, the GDPR in its terms, rules, scope of application, territorial, and jurisdictional range is overwhelmingly broad. The reason for such broadness is that it wants to regulate and ensure the safety of personal data by trying to fill out every possible loophole a violator might exploit now or in the future. However, this broad approach with its complexity has drawbacks. It caused establishments and member states to come up with several different interpretations of these rules, which in turn indirectly limited the understanding of the data protection authorities' capacity to engage in prosecuting violators. Additionally, it opened the floodgates for meaningless claims and counterclaims that are backed by the vague and broad regulations that are tactically used to prolong litigations and drain out weaker parties' financial resources and time.

SECTION 2: The Imperfections of the GDPR

It is well known that objectivity is a two-way street. For this reason, after having thoroughly conducted an objective demonstration on how data protection and privacy regulations in Europe were developed, amended, regulated, and enforced nationally and internationally, we must take a look at the other side of this Regulation. Although the GDPR is dubbed as the gold standard in privacy regulation and data protection, it has its fair share of critics and doubters. This can be attributed to its relation to a subject of great magnitude, complexity, and influence on the macro, micro and meso levels of society. Accordingly, the following section will shed light on some of these downsides that are based on the different societal perspectives which constitute some facts, opinions of critics, and the accounts of those who have fallen as victims of this Regulation.

A- One-Size Fits All Policies.

It has been established that the GDPR has strengthened the largest companies and weakened start-ups and medium-sized firms. Those that are well-suited to abide by the GDPR are companies that have money to build suitable data protection frameworks and regularly update them to comply with the new set of regulations. Medium and small-sized businesses aren't

financially equipped to do so, and could potentially face fines and penalties for lack of protection on par with the GDPR. Additionally, users have become less likely to risk their privacy and data by trying out new platforms with uncertain protection levels and prefer to stick to what they think they know is "safe"[179]. For these reasons, companies such as Facebook, Google, Amazon grew their monopolies, acquired medium-sized companies that can't offer protection, and posed threats, which caused an increase in their market shares in the EU. It was evidently demonstrated through the perceived loss of one-third of market positions inflicted upon small and medium-sized ad-tech competitors[180].

From an American perspective, retailers, gaming companies, service provides, and media news outlets no longer operate physically or virtually in the EU. Reasons for that are attributed to their unpreparedness, or the inability to economically or legally abide or subject their users to these regulations. They preferred to self-censor rather than bearing the cost of adopting the GDPR with the risks it presented. Self-censorship of several U.S. websites and new media outlets denied access for European citizens since they would be subjected to the GDPR. For example, companies such as Valve, Uber Entertainment, Gravity interactive, Brent Ozar Unlimited, Payver, and many more American-based companies, websites, and newspaper establishments closed down in the EU[181]. While it was evident that the GDPR helped to increase barriers on the U.S.'s free-flow- open-border transfers policies to encourage and promote European companies and startups, it also made life difficult on the same European companies it wanted to help. Finally, one could point out that the historic €50M fine on Facebook is mediocre compared to its quarterly revenues, but the same type of fine relative to a medium or small-sized industry could prove costly.

[179] Roslyn Layton, The 10 Problems of the GDPR, Testimony, published by the American Enterprise Institute, March 12, 2019, page 3, found at https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf visitation date 25/8/2020.

[180] Mark Scott, Laurens Cerulus and Laura Kayali, Six months in, Europe's privacy revolution favors Google, Facebook, Article, published in Politico, November 23, 2018, found at https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/ visitation date 25/8/2020

[181] Layton (Roslyn), OP. Cit. supra note 179, pages 3,4

B- The Paradox of Free Speech v. the Right to be Forgotten Under the GDPR

In some ways, the protection of data and privacy under the GDPR's "right to be forgotten" came at the expense of the right to freedom of expression and free speech. The right to be forgotten gives data subjects the ability to request the erasure of their personal data from internet searches[182]. While this right provides benefits in regards to removing false, inaccurate, excessive, or abusive content and information, it creates a censorship cloak for many violators, offenders, and abusers to take advantage of. The negative aspect of data erasure would proliferate if its scope of application extended globally, as it was pushed on and supported by the CNIL in a case involving Google France[183]. This right was adopted in the ECJ in 2014, when a Spanish citizen who reacquired, his old home wanted to remove an auction notice for debt payment failure dating from 1998 on the website of a newspaper in Catalonia. He claimed that all past economical instabilities and payment issues had been resolved and that he shouldn't be still linked with them[184]. Fast forward to 2019, with the inclusion of this right under the GDPR, a case between Google and CNIL saw the CJEU protect the right to free speech by limiting its scope with the state rather than rendering it a global requirement. Google feared that a global implementation could set a precedent for authoritarian regimes to limit free speech and confine global internet application[185].

From an American perspective, the right to be forgotten clashes with the constitutionally preserved First Amendment freedom rights. It seems far-fetched for the American legislators and courts to accommodate the idea of legalizing de-listing or de-referencing as viewed by the European Union, even after what transpired regarding the recent CJEU ruling[186]. Many cases in recent times support this unwavering protection of the First Amendment such as *Broadcasting*

---

[182] GDPR, OP. Cit. supra note 2, Rec.65,66; Art.15,17

[183] Owen Bowcott, 'Right to be forgotten' could threaten global free speech, says NGOs, Article, published in The Guardian, September 9, 2018, found at https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos visitation date 25/8/2020

[184] CJEU, Google Spain SL, Case C-131/12, OP. Cit. supra note 135

[185] Bowcott (Owen), OP. Cit. supra note 183

[186] David Greene, European Court's Decision in Right To Be Forgotten Case is a Win for Free Speech, Deeplinks Blog, published September 26, 2019, found at https://www.eff.org/deeplinks/2019/09/european-courts-decision-right-be-forgotten-case-win-free-s#:~:text=In%20a%20significant%20victory%20for,by%20users%20around%20the%20world. Visitation date 29/8/2020

Corp. v. Cohn 420 U.S. 469 (1975) or *Manchanda v. Google, Inc. et al* , 2016 U.S. Dist. Lexis 158458, or *Garcia v. Google, Inc.*, 786 F.3d 733, 745–46 (9th Cir. 2015)[187].

From the perspective of journalists, it limits free speech and the freedom to get the needed information. Although they are exempted from some requirements of the GDPR for journalistic purposes under Art. 85. These exemptions still need to be adopted by the Member States and articulated in a manner that suits the laws of each state, which could be a long and harmful process for the industry. Additionally, as mentioned above, American media outlets, newspapers, and journalistic websites are either self-censoring or banned from engaging with EU citizens out of fear of inadequacy and sanctions[188].

Consequently, it is extremely difficult to form an equal coexistence between privacy rights, freedom of speech, and expression rights. It might have been possible previously, but in this day and age with the unlimited accessibility of information on the internet and the proliferation of blogs, e-articles, news websites it is hard to find a balance between these two rights.

C- Opt-In Fatigue for Consent and Legitimate Interest

The overwhelming number of cookie "pop-ups" or "Check the Box" after being subjected to multiple pages of unreadable small-sized font privacy policies that almost always need decoding, defies the real purpose of privacy protection. First of all, this process almost always ends up with users giving their consent without ever reading the privacy policies, or knowing the extent of the processing procedures. Even if companies adopt a better written, less sophisticated consent system, users would still opt to not read these terms[189]. Several factors could be in play here, for example, not providing consent doesn't allow the user to fully benefit from the application or website or device, or due to this modern era where everything is easily attainable and instant gratification is the norm rather than the exception, where users of the internet aim to get what

[187] Danielle Bernstein, Why the "Right to be Forgotten Won't Make it to the United States, Article in Michigan Technology Law Review, February 2020, found at http://mttlr.org/2020/02/why-the-right-to-be-forgotten-wont-make-it-to-the-united-states/ visitation date 29/8/2020

[188] Nani Jansen Reventlow, Symposium on the GDPR and International Law: Can the GDPR and Freedom of Expression Coexist? Article, Published in AJIL UNBOUND, Volume 114, January 2020, pp. 31-34 found at https://www.researchgate.net/publication/338407067_Can_the_GDPR_and_Freedom_of_Expression_Coexist#fullTextFileContent visitation date 29/8/2020

[189] Giles Cottle, A year of GDPR: blocked users, hot potato, and opt-in fatigue, blog, published June 18, 2019, found at https://deductive.com/blogs/year-gdpr-blocked-users-hot-potato-opt-in-fatigure/ visitation date 29/8/2020

they want as quickly as possible with minimal steps. Additionally, refusing to give consent will result in more frequent "pop-ups" or "check the box" to disrupt a user's web experience until he gives in a provides request, and the GDPR failed to explicitly address the abuse that companies could inflect through sending consent requests every time a page is opened[190]. For this reason, a different system is required to deal with the consent issues other than focusing on how the information is presented or requiring double clicks to obtain consent. It becomes a question of choice versus consent. Finally, the fear of abusing the ambiguous stipulation of legitimate interest drives small and medium-sized companies to over-use "pop-ups" and consent windows to stay on the safe side[191].

Other loopholes or negative consequences of GDPR include:

1-The borderless nature of the Regulation corresponds to the borderless nature of the internet and other technological proliferations. Thus, it created jurisdictional conflicts between states and countries that value control and protection over events that happen within their territory.

2-The time and money-consuming nature of litigation when going against big data companies. This also applies in the context of the previous point, for jurisdictional conflicts are bound to cost time and money.

3-The omission of device security regulations accounts for almost 6 billion connected devices[192]. Thus, rather than following a preventive approach to stop the root cause of unlawful data processing and cyberattacks, the Regulation was drawn up to act reactively to negligence misuse, and attacks. It followed the norm of fining violators after an infringement has been committed.

4-A lack of awareness building on data protection issues. This point correlates with the previous one since humans and their devices are the weakest links in any chain of protection. (Part two of the thesis will demonstrate how cybersecurity policies are built on awareness-raising.)

---

[190] Natasha Lomas, Most EU cookie 'consent' notices are meaningless or manipulative, study finds, Article, published on Tech-Crunch, August 10, 2019, found at https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/ visitation date 29/8/2020

[191] Michael Baxter, GDPR anniversary: has the regulation backfired? What next? Blog, March 27, 2019, found at https://www.information-age.com/gdpr-anniversary-citizens-custodians-of-data-privacy-by-design-trust-by-design-123482779/ visitation date 29/8/2020

[192] Ibid

5-The facial recognition programs that were not allowed in Europe but can be applied under the GDPR following user consent[193].

6-The broad and unspecific regulations surrounding automated profiling and inferred data as a product of surveillance, coupled with the fact that controllers aren't obliged to notify data subjects in regards to any profiling that takes place until it produces "legitimate impacts or comparably influences them[194].

7-The GDPR threatens innovation and research by being incompatible with big data, artificial intelligence, blockchain systems, and machine learning in fields of medicine, development, engineering, and entrepreneurship[195].

8-The GDPR followed a backward or upside-down approach to controlling privacy, since gaining better control over our privacy isn't attainable through better privacy policies and confusing data protection laws. To truly protect data control must be given to the users. Consequently, users can control what applications and services can access and for a specified reason[196].

These loopholes or disadvantages, whether based on opinions or facts and statistics, must be taken into consideration when objectively studying a newly implemented regulation.

In conclusion, whether the GDPR is deemed as a fortress for personal data or just a sandcastle, the ultimate undisputed fact remains that the GDPR is currently the leading regulatory framework for protecting the privacy of users and securing their data. Three years into the adoption and implementation of this law are still deemed as the infancy years of this Regulation. Thus, flaws, loopholes, and conflicts are expected and perceived as opportunities to further grow and modify this new regulation. Additionally, differences between Europe and the U.S. in their

[193] Kalev Leetaru, Will the EU's Data Protection Act Actually Lead to Less Online Privacy? Article, published May 8, 2018, found at https://www.forbes.com/sites/kalevleetaru/2018/05/08/will-the-eus-data-protection-act-actually-lead-to-less-online-privacy/?sh=678605cf355a visitation date 30/8/2020

[194] Optin Contacts, Loopholes in GDPR, Article, no date, found at https://www.optincontacts.com/blog/loopholes-in-gdpr/ visitation date 31/8/2020

[195] Layton (Roslyn), OP. Cit. supra note 179, page 6

[196] Mike Masnick, One Year into the GDPR: Can We Declare It A Total Failure Yet? Blog, May 24, 2019, found at https://www.techdirt.com/articles/20190521/17425842255/one-year-into-gdpr-can-we-declare-it-total-failure-yet.shtml visitation date 31/8/2020

approach, belief system, regulatory setup, and priorities will always put them on a crash course, but compromises and sacrifices need to happen to reduce collisions.

In light of what was discussed from a national, international, public, private, economic, and legal perspective. The real question remains to see whether these data protection and privacy regulations are leaving altering imprints or cracks in the fundamental principles of an equally sophisticated, data reliant, modern and autonomous branch of legal proceedings defined as Alternative Dispute Resolutions.

SUB-CHAPTER 2: Implications of Data Protection on ADR Methods (Arbitration)

ADR methods such as Arbitration, Mediation, and Conciliation are considered unique and specific procedures, that aim to provide remedies and resolutions for contracting parties or disputants. These procedures have been built on the preservation of relations, compromises, and bridging different perspectives. Accordingly, the cornerstones of extra-judicial processes are efficiency, consensual agreements, flexibility, and confidentiality with trust being their main anchor. The nature of these ADR methods, especially that of International Arbitration, involves multiple entities and persons and requires the handling of a multitude of personal data. Thus, extra-judicial procedures are subjected to data protection laws and privacy regulations at every level, which could further complexify their systems and may limit their autonomism. International arbitration is a data-driven procedure, where the processing of personal data is a core component of its make-up. Additionally, the digitalized nature of information made it impossible to overlook the confluence and impact of data protection laws on arbitration. The worldwide adoption of these regulations especially the GDPR makes them theoretically and practically applicable and consequential at every level of the arbitration. Accordingly, (Section 1) will study the theoretical application of the GDPRs main principles on International Arbitration. Whereas, (Section 2) will be a practical demonstration of how the rights and principles of data protection are integrated with arbitration.

SECTION 1: Theoretical Application of the GDPR on International Arbitration

The GDPR and WP29 (replaced by the EDPB) regulated and presented guidelines for several aspects related to the processing of personal data. By doing so, they presented data subjects with substantial rights and protections. These rights have directly influenced ADR procedures and court litigations. The question remains to see how far-reaching the applicability of the GDPR is on International Arbitration.

A- Supervisory Authority

According to Recital 20 of the GDPR, Member State courts and other judicial authorities are exempted from being under the supervision of the data protection supervisory authority. Instead, they remain under the supervision of the judicial authorities of the Member States themselves. The main reason behind such preclusion is to preserve the independence of the judicial procedures in task performance and decision-making[218]. By analyzing the terms used in Recital 20, arbitration isn't explicitly mentioned, but it does fall within the scope of data processing by "courts and other judicial authorities" mentioned in the Regulation. On these grounds, arbitration should be included in the exemption of not being supervised and monitored by data protection authorities, especially since it includes decision-making functions akin to those of the courts. However, for the exception to apply, DPA supervision should be substituted by judicial supervision, but court systems in EU Member States do not supervise arbitration procedures[219]. Additionally, Art. 55 of the GDPR doesn't mention arbitration when it declares the incompetence of supervisory authorities in information processing done by courts as within their judicial capacity[220]. Hence, arbitration remains under the supervision of the data protection authorities and isn't included in the exemption.

B- Exemption From Certain Rights

The GDPR offers several rights to data subjects intra/post-processing of their personal data. However, some of these rights- under certain circumstances- can be excluded from application. Article 23 of the GDPR, gave the Member States the ability to exempt certain processing activities from being deemed as violations due to obstructions on data subjects' rights. For these exemptions to apply, they must result from respecting the fundamental rights and freedoms and satisfy the necessity and proportionality principles in a democratic society that guarantee, among other things, the "protection of judicial independence and judicial proceedings" and "the

[218] GDPR OP. Cit. supra note 2, Recital 20
[219] Kathleen Paisley, It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration, Article, published in Fordham International Law Journal, Volume 41, Issue 4, 2018, pp. 841,931, page used 857, found at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2707&context=ilj visitation date 9/12/2020
[220] GDPR, OP. Cit. supra note 2, Art. 55

enforcement of civil law claims"[221]. For example, Ireland applied Article 23 and exempted several of the data subjects' rights from being applicable such as the right to access data, the right to rectify or erase data, the right to data portability, the right to restrict additional processing, and the rights of objection to automated decision making and transparency. The Irish Data Protection Bill excluded these rights on grounds found in the GDPR (Rec.52,111; Art.23), for what is "necessary and proportionate" to adequately fulfill requirements of establishing or defending legal claims or proceedings, whether ongoing or prospective; regardless of being presented before a court, statutory tribunal, body, or in an administrative or out-of-court procedure[222]. Therefore, since arbitration accounts as an "out-of-court" procedure, these exemptions apply[223]. On that account, these exemptions under the GDPR offer protection for data subjects on two fronts, they are compatible with international arbitration since it has a decision-making function of judicial aspects, thus preserving the capabilities and essence of litigations. Additionally, it secures the totality of the GDPR application.

C- The Scope of Application of the GDPR in Relation to International Arbitration

a) What constitutes as "Personal Data" in Arbitration?

It has been established that the GDPR has adopted a broad definition of "personal data". It includes any information relating to an identified or identifiable natural person. Accordingly, it could be information such as name, home address, email address, location data, cookie id, data held by doctors, physical, psychological, mental, cultural, genetic, or economic information about a person[224]. However, information such as a company's registration number or a company email address (info@company.com), or anonymized data, are not included[225]. Nonetheless, if the mentioned company or business-related information falls within the category of information that can identify or are identifiable of a natural person, they are included[226]. Consequently, information exchanged during an arbitration proceeding, whether witness statements, evidence,

[221] Ibid, Art. 23
[222] Irish Data Protection Bill (No. 10b of 2018), Art. 57(1)(a)(b); Art. 57(3)(a)(iv); Art. 57(7)(b), found at https://data.oireachtas.ie/ie/oireachtas/bill/2018/10/eng/ver_b/b10b18s.pdf visitation date 9/12/2020
[223] Paisley (Kathleen), OP. Cit. supra note 219, page 858
[224] GDPR, OP. Cit. supra note 2, Article 4
[225] EU Official Website, what is personal data? found at https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en visitation date 9/12/2020
[226] GDPR, OP. Cit. supra note 2, Recital 26

memorials, expert reports, the award, or even business-related information that identify or could identify a person, are classified as personal data under the GDPR[227].

b) What is defined as "Processing" of personal data in Arbitration?

Again, due to the broad and open-ended definition adopted by the GDPR concerning "processing", almost every action taken during arbitration procedures is considered as processing of personal data. The definition includes: "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data" [228], whether done manually or by automated means[229]. For example, the shredding of documents or note-taking practices that include personal information is within the GDPR. From an international arbitration standpoint, processing could be: document retention, review, destruction, or transfer to third parties; disclosing material or documents to other parties such as experts, councils, arbitral tribunals or institutions; award preparation, exchanges, issuances, etc. Moreover, "processing" under the GDPR in an arbitration context is a continuous activity that starts from the moment of retaining or acquiring personal data, until their destruction[230]. Finally, it is incumbent upon arbitral parties to handle and process data according to its defined status. Processing needs to satisfy a legal basis to be accepted under the GDPR, depending on the sensitivity of the data. Normal data processing needs to fulfill one of four main conditions: consent, conclusion or performance of a contract with the data subject, legitimate interest, or a legal obligation under the EEA law[231]. Sensitive data requires more complex requirements, with criminal convictions and offenses being at the top of that list[232]. Moreover, other principles apply such as transparency[233], proportionality, data minimization, storage limitations, data accessibility, correction, deletion, etc., [234]all of which need to be adhered to in arbitration.

---

[227] Paisley (Kathleen), OP. Cit. supra note 219, page 863
[228] GDPR, OP. Cit. supra note 2, Article 4(2)
[229] Ibid, Recital 15
[230] Paisley (Kathleen), OP. Cit. supra note 219, pages 864,865
[231] GDPR, OP. Cit. supra note 2, Article 6
[232] Ibid, Articles 9, 10
[233] Ibid, Articles 13,14
[234] Ibid, Article 5

c) Who is involved?

As mentioned in the First Part of this thesis, Article 3 of the GDPR addresses the territorial scope of the GDPR. It applies to the processing of personal data done by an establishment of a controller or processor in the EU, whether the processing takes place inside or outside the Union. Additionally, the GDPR applies even if the controller isn't established in the EU, but is bound by it through Member State laws under the umbrella of public international law. Moreover, the territorial reach of the GDPR applies to the processing of data subjects' data -who are in the EU- by controllers or processors outside the EU, when processing is related to the offering of goods and services, or the monitoring of their behavior within the EU[235]. By applying this article on international arbitration, each person involved in the processing activities must be accounted for[236]. This means that every arbitrator, institution, council, expert, witness, and other involved parties who processes data as previously defined, might satisfy the conditions of Article 3, thus becoming subject to the GDPR. For example, one of the three arbitrators could be established in the EU, so he/she must apply the GDPR. Similarly, parties involved may not be based in the EU, but the respective councils or relevant persons are, and since they process personal data, they become subjected to the GDPR. Another example is the International Chamber of Commerce (ICC) Paris, since it is established in a Member state, the application of the GDPR on its arbitration procedures applies. Hence, almost always a party involved in the arbitral process will have their data processed in a way that puts them within the confines of the GDPR. In turn, this may trigger the joint liability of controllers, especially in situations where one arbitrator is bound by the GDPR in an arbitral tribunal[237]. Finally, even parties that aren't part of the dispute, but are somehow related to the parties through employment contracts, business transactions, or any type of relationship that could potentially subject their personal data to processing in the context of ADR, will have actionable claims under the GDPR. However, they must satisfy the applicability scope of the regulation.

[235] Ibid, Article 3
[236] GDPR, OP. Cit. supra note 2, Article 3
[237] David Rosenthal, Complying with the General Data Protection Regulation (GDPR) in International Arbitration- Practical Guidance, Journal in 37 ASA Bull. No. 4/2019, published by Kluwer Law International, The Netherlands, pp. 822- 852 pages 823,824, found at https://www.rosenthal.ch/downloads/Rosenthal-ArbitrationGDRP.pdf visitation date 11/12/2020

d) What requirements apply in an arbitral context? (Accountability Principle)

The satisfaction of the previously discussed questions under the GDPR requirements, related to who processes; what is processed; and how processing happens, sets up the involved arbitral parties (mainly the arbitral tribunal or party councils) to attain controller or processor status. As a result, the GDPR's prescribed obligations for data controllers and processors apply in arbitration procedures[238]. Consequently, joint controllership liability becomes an issue for arbitrators or any group of controllers previously defined. For controllers to be jointly liable, they often share the "controller" role where they decide on the purpose of processing or its essential means. Joint controllership could occur even if the party only contributes to certain decisions, without having direct access to the personal data at issue. This means, that joint liability applies to joint controllers for violating the GDPR, even if the joint controller isn't exclusively subject to the GDPR, and the burden of proof for not influencing the controlling process rests with him. Additionally, joint controllers are required to conclude an agreement between them that specifies their individual liabilities for compliance with the GDPR, which should be shared with the data subject[239]. Usually, in arbitration procedures, the decision over the purpose of what is deemed processing under the GDPR is individually decided upon, but jointly administered by arbitrators, the parties, and their counsel[240]. Opposing arguments are in place, some reaffirm that only the arbitrators or a sole arbitrator possess such controllership over personal information in an arbitration procedure, so considering them as joint-controllers is doubtful due to the complexity of such question, the joint agreement conditions, and their respective independence[241]. An additional perspective is the fact that arbitrators independently conclude the proceedings, which leaves out other stakeholders from joint liability, but doesn't strip away their individual obligations as controllers. However, it is argued that the essence of international arbitration cannot conform to these ideas. First of all, the broad scope of definitions used under the GDPR for key elements of processing and the parties involved is directly applicable to the nature of arbitration as a consensual process involving different people and entities that jointly decide on

[238] GDPR, OP. Cit. supra note 2, Recital 74, Article 24
[239] Ibid, Rec. 79,146, Art. 4(7),26(3),82(3)-(5)
[240] Rosenthal (David), OP. Cit. supra note 237, page 825,826
[241] Martin Zahariev (Dimitrov, Petrov & Co.), GDPR Issues in Commercial Arbitration and How to Mitigate Them, Blog, published in Kluwer Arbitration Blog, September 7, 2019, found at http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/ visitation date 12/12/2020

the rules of the procedure, including- among other things- the role of arbitrators[242]. Second of all, rarely does the arbitral tribunal solely decide on the arbitral file. Decisions regarding Terms of Reference, copies distributed, retention period, evidence submissions, protective strategies, Redfern schedules, witness statements, expert reports, etc., are jointly and consensually taken. The fact that the arbitral tribunal has the final say, doesn't change the reality through which these decisions were agreed upon and taken by the stakeholders involved. Hence, it is believed that joint-controllership liabilities apply in arbitration, not just between arbitrators[243]. Nonetheless, it remains to be seen how these principles are practically applied through a case-by-case observation and analysis.

As a final remark, arbitrators could be considered as secondary data controllers, since the data acquired and processed by them during an arbitral proceeding was already processed within its actual and initial use, either by a contractual or disputing party or by any other controller deemed as the initial data controller[244].

D- Application of International Data Transfer requirements on International Arbitration

The previously discussed international data transfer policies set by the GDPR directly affect international arbitration, whether based on adequacy decisions (Art. 45), appropriate safeguards such as Standard Contract Clauses or Binding Corporate Rules, etc., (Art. 46), or derogations for specific situations such transfers that are considered as a necessity for the establishment, exercise or defense of legal claims (Art. 49). Accordingly, since international arbitration usually involves the transfer of documents and other forms of personal data to recipients in other countries, they must conform to the requirements of the GDPR. This process could be done by simply conducting transfers with countries that have attained adequacy decisions. Alternatively, it could be conducted by referring to the more complicated safeguards through SCCs or BCRs, in which the sender of personal data such as the council, who wants to send a submission to an arbitrator (data recipient) found in an inadequate country (e.g., U.S.), must require from the recipient to

[242] Switzerland's Federal Code on Private International Law (CPIL) of December 18, 1987, went into effect January 1st, 2017, Chapter 12, "International Arbitration", Article 182 found at https://www.unine.ch/files/live/sites/florence.guillaume/files/shared/publications/pil_act_1987_as_from_1_1_2017.pdf visitation date 12/12/2020

[243] Rosenthal (David), OP. Cit. supra note 237, page 827

[244] Paisley (Kathleen), OP. Cit. supra note 219, pages 870, 884

admit to a special type of data protection agreement provided for by the EC. These contracts or agreements must not be changed under the GDPR. A third way is to use one of the transfer derogations such as the "necessary for the establishment, exercise or defense of legal claims" exception. Nevertheless, the correct application of this provision stipulates that: disclosure is only limited to personal data necessary for the proceedings, the recipient must keep the transferred data confidential, and the transferred data must only be used for proceeding requirements and related actions (such as appeal) by the recipient. These stipulations and agreements have to extend to encompass all parties that have or might have access to personal data such as witnesses and appointed experts, which might add additional paperwork and complexities to a fairly fast-moving and efficient process. Moreover, the use of Non-Disclosure-Agreements (NDAs) and the confidentiality of the arbitration process helps in adopting this derogation. In this regard, it's noteworthy to mention the importance of using "protective orders" or "court orders" in the U.S. These orders constitute confidentiality agreements signed by litigation parties to safeguard personal data from Europe. They essentially cover business secrets, which were then evolved to include any kind of personal data[245]. Likewise, U.S. arbitration follows a similar format to ensure confidentiality through witness signed confidentiality pronouncements[246].

The aforementioned questions concerning the applicability of the GDPR on International Arbitration are deeply integrated within the fabric of what ADR proceedings are about. Although they could add complexities, require additional awareness, effort, and paperwork. The fact remains that the essence of arbitration and other methods revolve around flexibility and party autonomy. However, one must always consider that the scope of data protection laws is tailored around data subjects that are affected even though they aren't part of the dispute but happen to be employees of a disputing company or in a business or any type of relationship with the involved parties. Hence, exploring these queries from a practical standpoint at every level of proceedings would elucidate and offer potential solutions on the underlying struggles between data protection laws, rights of data subjects, and ADR mechanisms.

[245] The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition), January 2017, found at: https://thesedonaconference.org/publication/International_Litigation_Principles visitation date: 12/12/2020

[246] Rosenthal (David), OP. Cit. supra note 237, page 831

SECTION 2: The Procedural Application of the GDPR on Arbitration

This section constitutes the practical impact that the GDPR has at every level of arbitral proceedings.

A- Pre-Dispute Integration. (Pre-Contractual Agreements)

a) The Question of whether extra-judicial processes can be used to resolve GDPR violations (the right of data portability as an example)

The use of the data subject's right to data portability in an increasingly online digital environment is an important stepping stone needed to figure out whether ADR methods apply. Under the GDPR, data portability allows data subjects to obtain and reuse their data that was previously given to a data controller. They have the freedom to store, use, or transfer their data to another controller. In turn, controllers must provide the requested data in a "structured, commonly used and machine-readable format"[247]. Accordingly, portability can be achieved through several methods, either physically through hardware instruments, or using online means. Thus, data subjects have an enforceable right that allows them to transfer data, upon request, from one controller to another, without harming the rights and freedoms of others[248]. The integration of third parties or other controllers in data portability actions, coupled with the heterogeneous mixture of differently regulated personal and non-personal data (EU Non-Personal Data Regulation 2018/1807[249]) could widen the scope of bilateral disputes to involve interests and positions of third parties. In case of altercations or right infringements, Article 77(1) GDPR gives data subjects the right to submit a complaint with a supervisory authority without having "prejudice to any other administrative or judicial remedy"[250]. In turn, Article 79(1) GDPR emphasizes the idea of the effectiveness of a judicial remedy where violations of rights under this regulation occur without bias towards any non-judicial, administrative, or the

[247] GDPR, OP. Cit. supra note 2, Article 20(1)
[248] Ibid, Art.20(2), (3)
[249] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, L 303/59, published in the Official Journal of the European Union, 28.11.2018, found at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807 visitation date: 13/12/2020
[250] GDPR, OP. Cit. supra note 2, Article 77

supervisory authorities' means of recourse[251]. Thus, disputes resulting from non-compliance or infringement of portability rights fall under Articles 77 and 79. Additionally, the explicit reservation of non-judicial remedies shows the foreseen significance of these methods to resolve such disputes. Building on this, Article 40 GDPR promotes the self-regulatory adoption of codes of conduct to properly administer the provisions of the regulation and explicitly refers to "out-of-court proceedings and other dispute resolution procedures" to settle conflicts between data subjects and controllers that concern processing, while preserving the right to judicial remedies under Articles 77 and 79[252]. Hence, the consideration of ADR procedures to settle these differences becomes increasingly important and effective.

As demonstrated above, ADR methods are not excluded from GDPR application, and their dynamic, modern and contractual/consensual structure makes them adequately prepared to administer appropriate remedies. Furthermore, ADR methods offer preventive resolutions that could relieve judicial or administrative bodies from the overwhelming number of intricate disputes, especially those related to data portability in a highly digitalized online environment. However, achieving optimal enforceability and effectiveness requires the adoption of a uniform alternative dispute resolution mechanism to stop the fragmentation of disputes between judicial, administrative courts, and ADR methods. This approach could be used to avoid situations such as the one exemplified in infringing the right of data portability that could involve multiple unrelated parties, including different sets of personal and non-personal rights[253].

b) Secondary Processing

The processing of personal information during an arbitral proceeding constitutes secondary processing. By the time an arbitral proceeding occurs, personal data will have been initially collected and processed to fulfill an intended purpose in the context of an employment or business relationship between the involved participants or third parties. Under Article 6(4) GDPR, secondary processing must be in line with the original purpose of the initial processing.

---

[251] Ibid, Article 79

[252] Ibid, Article 40

[253] Jacques de Werra, Using Arbitration and ADR for Disputes About Personal and Non-Personal Data: What Lessons From Recent Developments in Europe, Article, published in the American Review of International Arbitration (ARIA), Volume 3, No.2 © JurisNet, LLC, 2019, pp. 195,217, page 202, found at https://www.digitallawcenter.ch/sites/default/files/publications/unige_134313_attachment01.pdf visitation date 12/12/2020

Thus, factors such as purpose compatibility, the contextual basis of collection, the relationship between a controller and a data subject, the nature of personal data, the future consequences of such processing, and the assigned safeguards, need to be considered[254]. Deciding on the legitimacy of secondary processing in arbitration and its relationship with the original purpose in company dealings and business relationships is a case-by-case study, especially since secondary processing will probably happen to personal data that belongs to subjects that aren't part of the arbitration, but happen to be linkable employees or in business or personal relationship with the involved parties. Hence, it is best to inform data subjects and acquire consent regarding possible processing in a future dispute before to the start of any proceedings[255].

c) Data Retention Issues

The GDPR considers data retention as processing. As a result, controllers are obliged to set retention periods on personal data at the time of collection[256]. This requirement may obstruct the proceedings of international arbitration since disputes may happen long after the retention period expires. Additionally, data retention principles aren't unified between country laws or sector-specific laws. For example, unanticipated disputes may occur between U.S. and EU companies each having different data retention requirements, especially that U.S. laws don't consider data retention as processing. WP29 addressed this issue in the Disclosure Guidelines under DPD. It mentioned the different time limits for bringing claims in different countries, and that EU controllers don't have a legal basis to store data indefinitely due to the possibility of a future U.S. litigation. Despite having "litigation holds" or pre-emptive retention of information and personal data, these exceptions apply for data related to legal claims that have been administered to courts or might be. Hence, WP29 claimed that depending on a foreseeable or mere possibility of litigation isn't sufficient on its own to bypass data retention requirements. Therefore, future arbitration disputes outside retention periods, don't satisfy the conditions of the exception, which may prove to be costly on evidence administration and the overall proceeding[257]. This issue

[254] GDPR, OP. Cit. supra note 2, Article 6(4)
[255] Paisley (Kathleen), OP. Cit. supra note 219, page 885
[256] GDPR, OP. Cit. supra note 2, Article 5(e)
[257] Article 29 Data Protection Working Party, 00339/09/EN, WP 158, Working Document 1/2009 on pre-trial discovery for cross border civil litigation, adopted on 11 February 2009, pages 7 and 8, found at https://www.gpdp.gov.mo/uploadfile/others/wp158_en.pdf visitation date 13/12/2020

should be initially addressed and assessed by involved councils, data protection teams, and involved parties to balance different rights and preserve the legality of proceedings.

d) Consent in future disputes

Giving clear and unambiguous consent by providing full descriptions regarding future disputes and the risks that they may hold is a precautionary method to ensure data controllers' compliance with the GDPR. Data controllers should address this issue before any contractual or business relationship is formed, since it provides a clear basis for freely given consent. According to WP29, consent alone is insufficient for delivering legal grounds for big processing activities during litigation, and in the same context, this can be applied to international arbitration. However, WP29 didn't fully diminish the effectiveness of consent on future disputes, but rather preserved the effectiveness of consent given by key players in a dispute. Moreover, consent could be a pathway to administer other GDPR principles, and it can always be withdrawn[258]. The fact remains that such issues are subjected to a case-by-case analysis.

B- Planning the Arbitration Proceedings (Contractual Agreements)

Going into this stage, it is important to be aware that the implementation of the GDPR occurs whenever any single arbitration participant is subjected to the Regulation. This calls for early preparation for an inevitable exposure to the GDPR.

a) Arbitration Agreement

Due regards must be given by parties to data protection laws when drafting their arbitration agreement. Companies and other establishments are reviewing previously concluded agreements to modify them or make sure that they are on par with the data protection regulation. Post-revisions or prior planning must expressly address issues and rights raised by the GDPR, especially aspects of international data transfers and deciding on the legitimate purposes for data processing[259]. Additionally, a notice of arbitration or reply to notice is recommended when a

[258] Ibid, pages 7,8,9

[259] ICCA-IBA Joint Task Force on Data Protection in International Arbitration, Roadmap to Data Protection in International Arbitration, Draft Protocol, February 28, 2019, page 6, found at https://cdn.arbitration-icca.org/s3fs-public/document/media_document/roadmap_28.02.20.pdf visitation date 14/12/2020

party notices that data protection laws could have a major impact on the proceedings, thus alerting everyone and setting a clear course of action for the remainder of the process[260].

b) Choice of Institution and Arbitrator

Both the choice of institution and arbitrator are subject to scrutiny when planning for an arbitration proceeding. This is because parties should consider whether or not this institution or arbitrator is from a country that has adequate levels of protection or is subjected to other derogations or safeguards. Several challenges occur, some of which are: the institution is under the GDPR but the parties are not, or the parties are from Europe but the institution or arbitrator isn't based there. This will create additional conflicts regarding the implementation of the law and may require parties to conform with the GDPR, and integrate standard contract clauses to facilitate and legally conduct transfers without violating the regulation and thus face significant fines[261]. Consequently, these challenges may interfere with the choice of arbitrators or the suitable institution in a way that may lead to the appointment of an arbitrator or institution based on whether they are or aren't subjects, or want to be subjected to the GDPR directly or via contractual clauses. Accordingly, the determination of suitable arbitrators will not be based on their legitimate credentials[262]. For example, countries such as the U.S., China, and Singapore that excel in arbitration and offer many qualified arbitrators or institutions haven't received adequacy decisions by the EU Commission[263]. Additionally, institutions outside the EU or organized under international law such as the Permanent Court of Arbitration (PCA) or International Center for Settlement of Investment Disputes (ICSID) may not be subject to the Regulation[264]. The exclusion of international organizations from the scope of data protection laws comes as a result of the privileges and immunities held in treaties or country-specific agreements, in addition to the special set of rules prescribed for the international organization itself.

From another perspective, arbitrators that are considered to preside over a dispute, and happen to be managed by an institution should be given a 'notice of disclosure' concerning their

[260] Paisley (Kathleen), OP. Cit. supra note 219, page 892
[261] CCA- IBA Joint Task Force on Data Protection in International Arbitration, OP. Cit. supra note 259, page 8
[262] Paisley (Kathleen), OP. Cit. supra note 219, page 892,893
[263] EU Official Website, Adequacy Decisions, found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en visitation date 10/5/2020
[264] ICCA- IBA Joint Task Force on Data Protection in International Arbitration, OP. Cit. supra note 259, page 8

personal data with parties seeking arbitration proceedings. In this context, arbitration institutions are arbitral parties and thus data controllers. Hence, any use, disclosure, or transfer of its arbitrator's personal data must be done under the data protection regulation.

c)Vendor selections and Compliance teams.

Vendors are usually selected based on their location and ability to facilitate data processing and procedural requirements under the GDPR. They aid arbitral participants in achieving compliance by taking the role of data processors which makes data controllers accountable for their actions[265]. Additionally, companies must demonstrate compliance with the GDPR through documenting decisions that are related to any type of processing with its material/territorial scope covered by the Regulation. In turn, small-medium establishments (SMEs) are exempted from some documentation burdens, but they are required to show equivalent and realistic compliance efforts[266]. Moreover, the GDPR requires the appointment of data protection officers (DPOs)[267] and when necessary, the preparation of a data protection impact assessment (DPIA) for high-risk types of processing[268]. Applying these requirements on arbitration suggests that a joint effort from arbitration parties, vendors, DPOs, and GDPR compliance teams are needed to ensure the satisfaction of the Regulation in the development and implementation of the arbitral process. An optimal collaboration will not be the norm in such procedures especially since each team will have a different set of priorities to protect. Hence, the flexibility of ADR methods is needed to strike a balance between ensuring GDPR compliance without hindering the essence of the arbitral process[269].

d) Claim Preparation

Claim preparation is done through reviewing events and factoring in evidence that led to the dispute, which is probably personal data. Accordingly, claim preparation is another term for secondary processing done by data controllers[270]. There are some noteworthy principles

[265] Ibid
[266] GDPR, OP. Cit. supra note 2, Art. 30, 30(5)
[267] Ibid, Art. 37; 39
[268] Ibid, Art. 35
[269] Paisley (Kathleen), OP. Cit. supra note 219, page 891
[270] ICCA-IBA Joint Task Force on Data Protection in International Arbitration, OP. Cit. supra note 259, page 8

applicable in agreement planning such as data mapping, purpose limitation, and data minimization which will be covered in the following segment of GDPR issues during arbitration

C- GDPR Issues During Arbitration

Building on what was previously established (pre-dispute issues, planning of the agreement, the appointment of arbitrators) the same rights need to be addressed but in a different way. Previously, arbitral participants needed to be aware of the scope of data protection laws by knowing whom it affects, how it affects, what it affects, and make certain that they address those issues. However, their requirements don't end there. Arbitral Participants must ensure the proper administration of the pre-planned and agreed-upon rights and principles even after the award has been issued. The accurate pre-recognition and planning of data protection regulations' integration aren't always fully achievable, or in some cases might be simply omitted. Thus, the same principles need to be covered and integrated during the arbitration proceeding, which could prove even more onerous on the flow of the proceedings since problems will have occurred. Accordingly, the protection offered to participants under the GDPR will not have a precautionary and preventive characteristic.

It's noteworthy to mention that for a relatively fluent flow of arbitral proceedings that minimizes overlapping obligations and dysfunctionalities amongst participants, involved parties should assign the required tasks for each member. This type of task delegation of who is the processor, who is the controller, and the possible joint controller situation, coupled with the type of data to be processed, and transfer policies should be addressed at the start of case preparation. It is in everyone's best interest to establish or follow a data protection protocol. Finally, if parties don't raise data protection issues, the arbitral tribunal should. The remainder of this section will show examples of implementation during arbitral proceedings with practical solutions

a) Fairness

During the process of arbitration, personal data processed could belong to individuals that aren't part of the proceeding. These data subjects could have been unaware of the possibility that their data might be processed in this context. The principle of fairness requires the administration of proper notices and the performance of assessments of the effect that processing has on unrelated data subjects.

For example, the exchange of emails or their submission as evidence during any stage of arbitration, could identify individuals who are employees of both, either or none of the disputing parties. Due consideration should be given by involved parties and their councils regarding any type of document presented. It should be assessed whether data subjects expected processing in this context; how processing affects them and assess the processing's justifiability under these circumstances. The fact remains that fairness principles apply in light of the nature of personal data inspected and its purpose in arbitration. Pseudonymization or redaction also remain viable options.

b) Lawfulness of processing

As established, arbitration proceedings are infiltrated with copiousness of different types of data that could be from different countries and is case-specific. Additionally, the diverse lawful bases for processing that exist under the GDPR is dependent on the nature of personal data (sensitive or not) and its movement across borders or geographical location (inside the EU, countries with adequacy decisions, the existence of proper safeguards, established through exception and derogation). Thus, processing done in the context of arbitration should be administered and fulfilled under the data protection regulations for lawful processing.

For example, parties submit evidence and documentation in different forms such as emails, work-related statements, submissions, contractual agreements, etc., that hold personal information of different categories under the GDPR. Accordingly, processing should happen in relation to the prescribed obligations needed for each one. Most times, the document itself isn't the "personal data", but words (names, emails, numbers, religious beliefs, health issues, prior convictions), and phrases inside it make up personal data. Thus, due to the contrast of data categories held within a single document, taking the document in its entirety isn't recommended, and could amount to unlawful processing. This issue can be solved through identifying documents in the initial stages of the arbitral proceeding and administering the proper requirements of legal processing whether through legitimate interest or necessity based on legal claims or additional consent. However, relying solely on consent isn't advised where the system provides other means to achieve legal processing.

c) Data minimization

The applicability of this principle is important when selecting, producing, and disclosing documents.

Parties and their councils should check the relevancy of hardcopy documents and e-documents to the proceeding, and limit the volume of data collected to what is essential through applying filters related to the relevancy of data, people directly involved, and date ranges such as specified timeframes. These measures help prevent them from going back indefinitely in time and limit their exposure to locational boundaries. Additionally, where data is transferred outside the EU to a country that doesn't have adequacy decisions, arbitration parties should consider limiting the amount of data before transfers so that they could avoid unnecessary additional risks.

d) Purpose Limitation

Usually, when a person is hired in a company as a partner, executive, or in any position, before leaving the company, they will be informed that their data will be processed under normal job title-related matters when necessary. The purpose limitation principle applies in the event of an arbitral dispute that later arises, in which this person's work-specific related data is being further processed which covers attended meetings, emails exchanged, or papers signed. It becomes within the scope of the processing notice that that person consented to in relation to their job description.

e) Data Subject's rights

Rights such as data access, modification, withdrawing consent, objection to processing, and erasure can be requested by the data subjects concerning the processing of their data. In an arbitration context, such requests can be made to the tribunal or the opposing counsel to access their data which was processed during arbitration. The party who receives the request has 30 days to address the request unless extended. However, the validity of these requests is conditioned by not adversely affecting the rights and freedoms of others, and aren't exempted under national laws. Thus, not all documents could be provided where they satisfy these derogations. Complications arising from such rights remain case-specific and could be mitigated in the arbitration planning phase or through a data protection protocol that addresses these issues.

f) Data security

IBA Cybersecurity Guidelines specifically addressed these issues (this subject will be explored in the following chapter). The fact remains that the application of a proportionate, risk-based approach to information security is needed. More importantly because of the frequent interactions, public web utilizations, lack of encryptions, and constant movement of people and their personal data in an environment infested by cybercriminals. The lack of cybersecurity measures could prove costly on arbitral proceedings if data security isn't administered properly, and can be counterproductive if excessively administered.

g) Transparency

The application of the transparency requirement could be a daunting task, especially since is subjected to several considerations and exceptions. As with most requirements and principles, transparency is case-dependent. For example, the collection of emails as evidence from a small number of employees in the search of relevant case-related information will potentially hold the personal information of a huge number of people. Under transparency requirements, these data subjects should be given notice and consent to the processing. However, getting a hold of these data subjects, especially when they are unrelated or distant from the controllers and processors is a challenging task. It is in the best interest of everyone involved in the arbitral process to include clear transparency requirements applicable to all levels of the proceeding, and be flexible enough to include later data acquirements under different consent purposes.

h) Utilization of service providers

It is common practice for arbitral participants to appoint private contractors, data platform service providers, translators, transcribers, experts (e-discovery professionals); as well as engage with ad hoc tribunal secretaries and acquire arbitral institutional aids. Accordingly, these service providers may be controllers in the context of their work, or processors appointed by arbitral controllers and work under their instructions. Accordingly, role designation and data protection obligations apply, especially those under the cross-border data transfers since data will be transferred to these third parties and joint controllership liabilities

D- Orders, Decisions, and Awards

Although arbitration is confidential, awards and other decisions are often made public. This could happen in countries where the enforcement of the award happens through the judicial authority, or in investment and treaty-based arbitration, where awards are publicized and commercialized through institutions. However, parties could request redactions, challenge the decision, or object to the publication of the award. Accordingly, decisions or awards in the context of data protection laws most certainly contain personal information of different categories (normal personal data, sensitive data). Moreover, due to the wide scope of personal data defined under the GDPR, redaction of sensitive data or data that directly identifies a person will not suffice. Data subjects will still be identifiable through the award, order, or decision. Thus, arbitrators and institutions should jointly address these issues early on, and devise a way of rendering awards that are in line with the requirements of the data protection laws.

E- After the Arbitration- Retention/Deletion

Since data retention and deletion are considered processing under the GDPR, arbitral participants should follow retention protocols that are suitable for balancing data subjects' needs with what is required in the context of an arbitral process. For example, controllers during arbitration should retain data for a period that is justifiable, reasonably necessary, and under the purpose for which data subjects were given notice of and consented to[271].

To conclude this section, some key takeaways from applying data protection regulations and principles on arbitration proceedings are:

1-Data Protection Regulations apply to individual data subjects, not parties alone.

2- The Regulations apply to arbitral participants and data subjects, not to the process of arbitration itself.

[271] Information in this section especially from "C- GDPR Issues During Arbitration" and onward are collected from: The ICCA-IBA RoadMap to Data Protection in International Arbitration; The Sedona Conference: International Principles for Addressing Data Protection in Cross-Border Government and Internal Investigation: Principles, Commentary & Best Practices; ICC Rules concerning the protection of data; London Court of International Arbitration Rules.

3-Data Subjects' rights under the data protection regulations can't be waived by arbitral parties.

4-Application of data protection rules is party and data subject-dependent, fact-driven, and done on a case-by-case basis. Thus, considering a single set of procedures for different cases isn't recommended.

5-Early planning, discussions, and agreements on all facets of the application and limitations set by data protection rules and regulations are of the utmost importance. Failure to do so might result in violations of the regulation causing harsh fines and sanctions (up to €20M or 4% of revenue) to be applied. From another perspective, it could be used tactically by parties to disrupt the flow of the proceedings by raising data protection issues later on when parties are in a losing situation such as withholding evidence due to data protection concerns after the other party submitted his.

6-Under good case management practices, arbitrators should raise all data protection concerns and security issues, on their own and when parties fail to do so.

Application of data protection regulations is a demanding task for everyone involved, whether through taking extensive precautions, dealing with the multitude of data subjects involved, requiring additional paperwork, documentation, or following up and ensuring practical implementation throughout. Hence, if not administered and managed properly, proportionately, and adequately these regulations could risk the specificity, legitimacy, and flexibility of the proceedings.

How societies approach and regulate data protection and privacy dictates the future trajectory of human civilization, in this age of surveillance capitalism[272], unrestricted accessibilities, unforeseen cybercrimes, and global interconnection. When faced with the unprecedented, one

[272] Shoshana Zuboff, The Age of Surveillance Capitalism, first published by Profile Books Ltd, 1st Edition, London, 2019, page 11 "The Definition"- Surveillance Capitalism: " A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; 2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification; 3. A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history; 4. The foundational framework of a surveillance economy; 5. As significant a threat to human nature in the twenty-first century as industrial capitalism was to the natural world in the nineteenth and twentieth; 6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; 7. A movement that aims to impose a new collective order based on total certainty; 8. An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty".

can't resort to previously practiced methods or already established principles and expect victory. It has come to a point that people's data have become the basis for product selling. This means that we have become the products that big data companies use. Our privacy is being violated and our data is being used and sold to other companies to make products based on the data they unlawfully acquired, then we buy those things. So, it has become a cycle of offering services to breach privacy, mine and sell data for profit, make other services based on that previously acquired data to make further profits, and to resell them to the same people for even more profit[273]. Frankly speaking, how is that any different from human trafficking or the notion of slave auctioning long ago, but rather than selling or offering up the physical body, this time it's the mental and intangible side of humans that is being sold. Hence, the concept of privacy and data protection needs to be perceived and regulated from a different scope.

Keeping that which was explained in mind, establishing a full-on safe and carefree environment for data subjects doesn't solely rest on the right application of data protection laws. Another crucial side of achieving ideal protection in this digital and online-driven age rests with the establishment and proper functionality and use of information technology and cybersecurity measures.

[273] Ibid, examples on the use of unlawfully obtained data to sell them and make profits are present throughout the book. Such as those committed by Ford, Facebook, Apple, etc.

PART 2: The Ramifications of Global Digitalization on ADR

Our modern civilization has become deeply and essentially network and internet dependent. This dependency applies to our daily lives at the narrow scope of using phones, laptops, etc., and at a wider scale manifested in every major sector such as the legal, governmental, communications, health, banking, and manufacturing. Additionally, the technological and virtual reality takeover has been expressed through smart cars, smart cities, and cryptocurrencies, which will present key future issues and opportunities. The manifestations of digitalization have completely changed the dynamics of our society. The traditional judicial and extrajudicial systems will not be able to cope with the new demands of the digital age. Thus, new demands must be met with new supplies, and new problems require a new way of thinking outside the confines of traditional concepts. Accordingly, online dispute resolution methods offer that virtue. It is a consequence of the digital age and at the same time presents a remedy for today's problems. For this reason, (CHAPTER 1) will be dedicated to the exploration of ODR and the adaptability it conveys when dealing with the challenges of the digital age. However, by itself, ODR isn't a solution. The global dependency on digitalization is a facilitator, but it makes everything in our world susceptible to cyberattacks. Accordingly, the main issue becomes a matter of procuring cyber-safety rather than just cybersecurity, which if not dealt with could endanger our lives and not just our data. With that being said, nearly all major sectors in almost all markets have experienced, either directly or indirectly, serious cyber security issues, with no evident sign of this trend slowing down anytime soon. Nonetheless, the first step towards gaining control over cyberspace starts with mastering cybersecurity. Consequently, (CHAPTER 2) will delve into some aspects of cyberspace such as the nature of its crimes, its influence on ADR, and the remedies being offered by international actors (Cybersecurity Protocol for International Arbitration). Thus, ADR's specificity is raised again at a more intricate and foundational level when it faces off with IT integration and the laws of cyberspace.

CHAPTER 1: The Modern Digitalization of Extra-Judicial Functions

The virtual world has become more than just an extension or accessory of the real world. Its influence on states, organizations, and people is spawning a new set of obstacles and issues that need addressing. However, it has also provided suitable remedies that match the conflicts created by the digital era. In that sense, the incorporation of information technology with ADR methods, especially Arbitration, has been accounted for in the arbitration community. Additionally, COVID-19 has caused a total dependency on online mechanisms, which added to the relevancy of exploring this subject. With that being said, IT integration in extra-judicial and judicial systems has gained popularity. It shifted from a luxurious accessory that makes work easier, to an absolute necessity needed for the continuity and proper functioning of the sector. On top of that, some are willing to go as far as to reaffirm the notion of AI superiority on humans, just like in any labor or manufacturing operation. For this reason, the following chapter will explore the different sides of the modern digitalization of extra-judicial systems, which goes beyond ITs' impact on Traditional ADR, and explores one of its products manifested through ODR (Sub-Chapter 1) Whereas, (Sub-Chapter 2) will consider issues manifested by the digitalization of ADR and the novel ingenuities such as Artificial Intelligence.

SUB-CHAPTER 1: Online Dispute Resolution

Information technology has become an essential part of the legal profession. The use of electronic means to produce, obtain, modify, store, transfer, and remove information has become easier, more efficient, and faster. Thus, creating a suitable environment of IT burgeoning in the information-dependent and flexible nature of dispute resolution procedures. The integration of IT in this domain can be studied on two levels: IT in traditional offline dispute resolution procedures, and in online dispute resolution procedures. The focus of the thesis as a whole was centered around how IT and its many uses and forms can influence traditional offline ADR methods. However, cyberspace and IT tools could be perceived from another perspective, which is beyond the simple addition of technological tools that have consequences and impacts or offer remedies to traditional methods. Through digitalization and IT came the creation of a modified system of dispute resolution that operates in cyberspace. (Section 1) will give an overview of ODR. Whereas, (Section 2) will show the importance of ODR through a comparison with ADR.

SECTION 1: Online Dispute Resolution: A Result and a Consequence of the Digital Era

- *Overview of IT use in Traditional Arbitration*

The shift from ADR to ODR didn't happen overnight. An important distinction has to be made between traditional ADR methods that use the internet and other IT tools with purely online dispute resolution methods that are initiated, concluded, and enforced using digital tools in cyberspace. The blueprints of this transition were informally adopted by ADR practitioners before the mid-90s as information booths or intermediary platforms of information for people. Following that, informal online disputes resolution mechanisms began to gain recognition, especially in the U.S. They were regarded as different mechanisms from traditional ADR and became an industry in 1998. Accordingly, experimental projects such as the Virtual Magistrate and the Online Ombuds Office were initiated[1]. In the early 2000s commercial sites offering ODR services in the U.S. such as "Cybersettle", "SquareTrade", "SmartSettle" and "The Mediation Room" that perform different functions became popular.

[1] Mohamed S. Abdel Wahab, Ethan Katsh & Daniel Rainey, Online Dispute Resolution: Theory and Practice, Eleven International Publishing, The Hague, Netherlands, February 2013, Chapter 1 page 23, found at https://www.mediate.com/pdf/katsh.pdf visitation date 15/2/2020

The integration of IT in offline ADR is centered around its most common uses for average practitioners with a standard understanding of IT. Accordingly, the use of IT can include emails and other electronic communications between involved parties, data storage using portable or fixed storage media (e.g. flash drives, DVDs, hard drives, and cloud-based storage), computer software; programs that allow parties to present their cases through online filing rather than using a paper format, case-management websites, and hearing room technologies (e.g. videoconferencing, multimedia presentations, translations, and "real-time" electronic transcripts)[2]. The movement towards regulating this form of IT integration was done through the ICC (International Court of Arbitration) Commission on Arbitration and ADR's Task Force on the Use of Information Technology in International Arbitration[3]. Consequently, the international arbitration community began to welcome the use of IT in international arbitration at an increasing rate, especially due to the advances in technology and maturity in utilization amongst people. Thus, operations that were previously far-fetched or lacked proper logistics to figure out and conclude became easily accomplished with IT tools. For example, there was a noticeable difference in the way correspondence between the involved parties was concluded. In 2004, correspondence exchange was done by email, but it was also sent by post or an overnight courier service. Nowadays, upon tribunal constitution, written communications are mainly done through electronic means in an electronic format (e.g., Portable Document Format or PDF). Additionally, in 2004, the use of file transfer protocol servers to transfer large submissions to other parties and the tribunal was seldom used, because initiating and correctly performing the process was a difficult task. However, using today's technology in transferring information has become more common through readily available and easily accessible bulk file hosting services utilizing FTPs (e.g., Dropbox, Google Drive). Moreover, at the beginning of the IT employment movement, users in this domain tended to focus on the formation of a safe, private, and flexible "virtual data room" to serve as an online file repository. These "virtual rooms" would allow parties, arbitrators, and involved institutions to

[2] Gabrielle Kaufmann- Kohler, Thomas Schultz, The Use of Information Technology in Arbitration, December 2005, page 1, found at https://lk-k.com/wp-content/uploads/The-Use-of-Information-Technology-in-Arbitration.pdf visitation date 2/1/2021

[3] The Task Force on the Use of IT in International Arbitration was formed in 2002 and produced four documents in 2004: "Issues to be Considered when Using IT in International Arbitration", "Operating Standards for Using IT in International Arbitration (The Standards)", "Explanatory Notes on the Standards" and "IT in Arbitration: The Work of the ICC Task Force". This report updates the first of these four documents, "Issues to be Considered when Using IT in International Arbitration". Documents can be found at https://library.iccwbo.org/

have continuous and real-time access to files, correspondence, and other submissions. As a result, platforms for these purposes such as the ICC's "NetCase" in 2005[4]; the American Arbitration Association's (AAA) "WebFile"[5]; and the Arbitration and Mediation Center of the World Intellectual Property Organization's (WIPO) "Electronic Case Facility- ECAF"[6] were established. Nevertheless, even with the ICC working to develop and modify its internet-based cases management service, the emphasis on having these platforms decreased because of the availability of other means. Users today are depending on general-purpose and commercial services, such as Google Documents, to exchange and store documents. While oftentimes, such services are free, offering service providers with rights of access, use, and data analysis that could compromise the confidentiality, data integrity, and security through complicated general terms and conditions[7].

For reasons such as vast integration, increased dependency, and the nature of IT tools, coupled with people's ability to communicate with each other instantaneously across the globe, altered the essence of disputes. Those that were traditional disputes became mainly of a cross-border nature, and a new kind of disputes emerged, which is borderless. Consequently, anyone with internet access can become part of a business transaction with someone they have never met, or can become part of an online platform that will use their data. In turn, this dramatically increased the number of disputes, the majority of which are of low or medium value, that don't have an available or viable route of resolution proportional to the value of their disputes. These difficulties can be attributed to the inadequacy and unpreparedness of traditional forms of dispute resolution mechanisms to resolve the newer disputes. Thus, the need for a modern system that adapts to the modern ways of business transactions and can resolve borderless disputes of any value or nature has become clear. Hence, ODR came to fruition. It is the result of dispute evolvement and their transition from the actual world to the virtual realm, which in turn demanded the same transition from ADR to ODR.

[4] International Chamber of Commerce (ICC) Commission on Arbitration and ADR Report: Information Technology in International Arbitration, published and printed in October 2017 by Imprimerie Port Royal, Trappes (78), page 2, found at https://iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf visitation date 3/1/2021

[5] Found at https://adr.org/

[6] Found at https://www.wipo.int/amc/en/ecaf/introduction.jsp

[7] ICC Report, OP. Cit. supra note 4, pages 2,3

A- Defining Online Dispute Resolution

ODR is the combination of ADR and Information Communication Technology (ICT). Several terms have been used to label this mechanism such as, but not limited to, "Technology-Mediated Dispute Resolution" (TMDR), "Online ADR" (o-ADR), "Electronic ADR" (e-ADR), "Internet Dispute Resolution" (IDR), and other terms that include the words "virtual" and "cyber" as prefixes to the traditional means of dispute resolution. The original purpose of ODR was to resolve disputes occurring online, for such disputes didn't have available dispute resolution mechanisms or such mechanisms were inadequate[8]. Accordingly, ODR started as an online adaptation of ADR, and it was exclusively deemed by scholars as ADR supplemented with ICT tools[9]. Then a broader definition was used that incorporated online litigation and other sui generis (of their own kind) forms of dispute resolution into ODR, which were assisted by ICT[10]. However, ODR was narrowly described internationally to only include extra-judicial online dispute resolution. Thus, ODR is a new and modified version of ADR adopted as a result of the demands imposed by the virtual world. The purpose of ADR is to offer remedies and resolutions for disputes outside courts, so ODR is an online extra-judicial manifestation of the digital world that aims to achieve the same result[11].

Nonetheless, although ODR is a modified version of ADR, the merger of ADR with IT isn't only a transplant, but it is a form of synergy that makes ODR unique in its own sense[12]. In addition to the capability of ODR methods to resolve small and medium online disputes (e.g., e-disputes, e-commerce issues), it is also capable of resolving offline and large value disputes. For example, this is demonstrated through the operations of "Cybersettle" and "clickNsettle" as online service dispute resolution providers. In other words, ODR can be used to solve any type of dispute, whether online or offline. But, ODR is better suited for cases that originate in cyberspace, for the use of this mechanism helps in avoiding the complexities of determining the suitable jurisdiction. Additionally, online arbitration is more useful in resolving domain name disputes and intellectual

[8] Ethan Katsh, Online Dispute Resolution: Resolving Conflicts in Cyberspace, San-Francisco: Jossey-Bass, USA, May 2001, page 9

[9] Colin Rule, Online Dispute Resolution For Business: B2B, E-commerce, Consumer, Employment, Insurance, and other Commercial Conflicts, John Wiley & Sons, September 2002, page 44

[10] Gabrielle Kaufmann- Kohler, Thomas Schultz, Online Dispute Resolution: Challenges for Contemporary Justice, published in Kluwer Law International: The Hague Zurich, 2004, page 5

[11] Rule (Colin), OP. Cit. supra note 9, page 43

[12] Julia Hörnle, Cross-Border Internet Dispute Resolution, Cambridge University Press, New York, USA, February 2009, page 76

property disputes in cyberspace[13]. The protection of intellectual property online requires the presence of professionals in this field with technological expertise, which will increase the efficiency of resolution. These traits might not be available in normal judges or a jury that will rely only on civil and criminal sanctions, in addition to bearing extra costs on resources and time teaching them about the technological technicalities of the case[14]. ODR can be used to resolve family disputes, employment disputes, and commercial disputes as well as those with cross-border elements[15]. Moreover, the dependency on ODR has increased over the years, because it is better suited for resolving monetary disputes such as credit card issues and insurance claims that involve multiple economic transactions, usually between strangers with no prior interaction or relationship. In other words, ODR is more suitable in cases that involve multiple entities in several corners of the world with no prior relationships, which include numerous economic transactions, since they complement cyberspace's nature and function accordingly. However, cases that are based on family law and taxation law aren't suited for ODR, since they are bound by higher legal constraints and states are more rigorous in preserving their jurisdictional sovereignty in these matters[16].

The formulation of a fine line between ADR and ODR is dependent upon the role and impact that ICT tools have on the process since it is common to use smartphones, laptops, emails, and other means of technology that utilize cyberspace in ADR. ODR has evolved beyond the inclusion of emails and online forums in dispute resolution. Nowadays, it is considered as a technically sophisticated software capable of conducting administrative functions in cyberspace that was previously done offline. The majority of the dispute resolution process is handled and concluded online. This means that functions such as filing for a dispute, party agreements, communications, hearings, submission and evaluation of evidence, and even rendering settlements are done online.

---

[13] Aashit Shah, Using ADR to Solve Online Disputes, Article, published in Richmond Journal of Law & Technology, Volume 10, Issue 3, 2004, pages 3-5 found at https://jolt.richmond.edu/jolt-archive/v10i3/article25.pdf visitation date 15/4/2021

[14] Richard Michael Victorio, Internet Dispute Resolution (iDR): Bringing ADR into the 21st Century, Article, published in Pepperdine Dispute Resolution Law Journal, Volume 1: 279, 2001, pp.279-300, pages used 298-300, found at https://law.pepperdine.edu/dispute-resolution-law-journal/issues/volume-one/15-victorio.pdf visitation date 15/4/2021

[15] Pablo Cortes, Online Dispute Resolution for Consumers in the European Union, published by Routledge Research in IT and E-Commerce law, London and New York, 2011, page 2

[16] European Commission, Patrick Van Eecke, Maarten Truyens, EU Study on the Legal analysis of a single market for the Information Society: New rules for a new age? November 2009, published by DLA Piper UK LLP, July 22, 2014, Chapter 11, page 12, found at https://op.europa.eu/en/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722# visitation date 15/4/2021

Hence, ODR can be defined and differentiated from ADR through the influence of technology that acts as a fourth party in the process.

B- The Role of Technology as a Fourth Party in Dispute Resolution

The contribution of ICT tools and their influence on alternative dispute resolution has earned it the status of a fourth party by Ethan Katsh in 2001. It's an addition to the traditional three-sided structure made up of two parties involved in a dispute and a third neutral party. This could be attributed to the fact that the resolution of a dispute in ODR is not only performed by physical humans, but also by computers and software that independently contribute to the management of the dispute[17]. The virtual world offers an additional experience that doesn't need physical meetings or interactions. The tools used in communicating virtually have an impact on the way information and messages are transferred, conveyed, and understood by the parties. ICT can take on different roles in the process, it can act as a fourth party facilitator used by the involved parties in communications and other areas in the dispute. Additionally, but to a lesser extent in the present time, it can replace the neutral third party (which will be discussed later on in this chapter). In the former description, ICT is utilized in simple tasks such as information organization, altering the format of writing between parties which makes them more polite and constructive, stopping offensive or unnecessary bad or provocative language, sending out automatic responses to keep parties involved and engage by setting up meetings and reminders. Moreover, it can be used in more difficult tasks like evaluating and storing information, structuring the presentation of issues and statements, constructing a personal profile of each disputant, predicting outcomes, promoting brain-storming, and aiding parties in prioritization[18]. Furthermore, integrating ICT tools as a fourth party has had a transformative influence on traditional ADR processes. It established new dispute resolution mechanisms, such as blind bidding negotiation, which is a form of automated negotiation used to determine economic settlements for claims in which liability is not challenged; it could be perceived as a type of auction mechanism where information about the players' bids is mostly hidden. This procedure has no equivalent in the real-world[19]. The fear of ICT, as a fourth

[17] Katsh (Ethan), Rifkin (Janet), OP. Cit. supra note 8, page 93
[18] Ibid, page 129
[19] See https://www.worldarbitration.center/on-line-disputes/#:~:text=This%20is%20a%20negotiation%20process,the%20players'%20bids%20is%20hidden. Visitation date 16/4/2021

party, being an indispensable part of the process has grown significantly amongst ADR practitioners. Early on, some practitioners have criticized this notion because of ODR's lack of face-to-face interaction between parties, which would obstruct the development of ODR[20]. However, at this time, there is no alternative to ODR in resolving cross-border e-disputes and low-value disputes in a fast and cost-effective manner. Additionally, COVID-19 has proved our society's dependency on the internet and online tools, since individuals, organizations, entities, and even states that weren't well-equipped and proficient in functioning in cyberspace ceased their operations either partly or completely. Moreover, the argument in regards to the absence of face-to-face contact has become a primitive one, because the development of ICT tools gave secure, instantaneous, high quality, and cost-effective means of video conferencing through laptops and phones that could easily portray body language and emotions. Building on that, through the principles of contractual freedom and party autonomy, parties have the freedom to decide the type of ICT tools employed and those which are not permitted, depending on the nature of their dispute, and the technical capabilities of the parties[21]. This could limit and protect the process and their interests against the presence of any inequality that would disrupt the administration of a fair resolution. In other words, technology has advanced so much that it has several versions of the same tool suited for any human with different levels of technological capabilities and understanding.

SECTION 2: The Importance of ODR

To formulate a better understanding of the significance of ODR, it is important to look at the advantages and challenges of ODR, and those of traditional ADR methods. The following brief assessment of ADR processes will enrich the context of the study by playing the role of the second control group, after judicial litigation being the first. Thus, the positives and negatives of ODR are formulated based on a double comparison. Additionally, the COVID-19 pandemic has played a crucial role in showcasing the importance of ODR. Accordingly, to add further real-life context to this dissertation, the importance of ODR in the context of COVID-19 will be acknowledged.

[20] Joel B. Eisen, Are We Ready for Mediation in Cyberspace? Article, Published in Brigham Young University Law Review, Volume 4, 1998, pp. 1305-1360, page used 1311, found at https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=2824&context=lawreview visitation date 25/4/2021

[21] ICC Report, OP. Cit. supra note 4

Sub-Section 1: Traditional ADR v. ODR

A- Advantages and Drawbacks of Traditional ADR.

a) The Pros of ADR

Unlike normal litigation, there is a degree of confidentiality surrounding the process. Privacy and confidentiality are major contributors to the popularity of extra-judicial dispute resolution methods. It is especially important in commercial dealings that will preserve trade secrets and other important information that would jeopardize the business of a company if it were to become public knowledge. Accordingly, privacy and confidentiality allow parties to maintain their rivalry while simultaneously trying to resolve their disputes away from the public eye. Thus, it protects them from disclosures that would harm their interests, reputational status, and may impact all those who are involved directly or indirectly. Secondly, in comparison to normal litigation, ADR methods are cost and time-saving. This advantage increases the efficiency of the process since the strict legal formalities of litigation can be mentally, physically, and monetarily straining on the parties. One of the most important aspects that contribute to time and money-saving in the absence of appeals to arbitration awards. However, in recent times, the gap between ADR, especially arbitration and international arbitration, and legal litigation has significantly decreased in regards to time and money-saving. The complex nature of disputes, especially those that involve cross-border transactions and several entities, has increased the time and money spent in arbitration by disputants. Concerning costs of arbitration, the fees of arbitrators and experts multiplied by the hours spent in resolving the dispute compensates for the difference in cost between the legal requirements of litigation and arbitration. A "cost of international arbitration survey" conducted by the Chartered Institute of Arbitrators (CIArb) between 1991 and 2010, which included 254 arbitrators and data from several arbitral institutions (e.g., ICC, LCIA, AAA, etc.,) provides context to the aforementioned premise. It found that the overall average cost of international arbitration is around $2.6 million for claimants (the majority of which was attributed to legal fees- $1.6m to $1.8m) and about 10% less for respondents. Additionally, the cost of investment arbitration was higher and individual disputes could cost significantly less[22]. Moreover, these sums

[22] Chartered Institute of Arbitrators (CIArb), CIArb Costs of International Arbitration Survey 2011, pages 10,13 found at https://www.iaa-network.com/wp-content/uploads/2017/01/CIArb-Cost-of-International-Arbitration-Survey.pdf visitation date 18/4/2021

have increased after this survey (i.e., from 2011- till the present day) which was a result of inflation and higher costs of living. For example, on August 11, 2020, the LCIA released an update to its Arbitration Rules of 2014, increasing the costs of LCIA Arbitration[23]. The third advantage of ADR is its conciliatory function. ADR methods are voluntarily decided upon by parties and require their cooperation in determining the result. Through this function, ADR aims to allow the parties to acknowledge the dispute as a common struggle that needs a cooperative approach to resolve. Accordingly, the resolution of a dispute is mainly based upon finding common ground without obvious winners or losers. The end result defined by mutually accepted agreements creates a win-win situation for parties. It provides fair reconciliation that covers the needs and interests of both parties and doesn't burn down the bridge of future business relationships. In other words, ADR plays a game of positive-sum solution rather than a zero-sum solution[24]. Finally, ADR methods offer a great deal of flexibility and part autonomy. This is the result of the nature of ADR which doesn't include the same formalities and confrontational aspects of litigation. The parties are in control of the process, and they're free to choose the forum, arbitrator, type of procedure, etc. Additionally, the scope of flexibility extends to neutral third parties and the outcome of the procedure.

b) The Cons of ADR

First of all, it should be noted that ADR methods are for parties who seek to mutually resolve disputes, and aren't driven by avenging legal rights. The first drawback could be perceived from the parties' perspectives and their relationships. Being emotionally invested in a personal duel with the other party to the extent that could disrupt negotiations, and nullify the effectiveness of the process. Additionally, power imbalances between parties in the context of extra-judicial resolutions that are based on flexible agreements, bargaining capabilities, and informalities, would prove to be problematic in reaching compromises and mutually agreed-upon solutions. Moreover, since ADR methods rely heavily on party cooperation, it could cause difficulties in the execution and finality of agreements, especially in the absence of binding legal rules. This is hugely

[23] See https://www.lcia.org/Dispute_Resolution_Services/schedule-of-costs-lcia-arbitration-2020.aspx visitation date 18/4/2021

[24] Isabelle Manevy, Online Dispute Resolution: what future? D.E.A de droit anglaise et nord-americian des affaires, University de Paris 1, June 2001, page 9, found at http://lthoumyre.chez.com/uni/mem/17/odr01.pdf visitation date 18/4/2021

concerning in ADR forms that solely depend on voluntary compliance and cooperation in execution and enforcement[25]. Another portion of drawbacks can be concluded from the nature of some ADR procedures. Some procedures often lack procedural or constitutional safeguards provided in normal litigation. The absence of safeguards such as the right to a jury and the right to counsel decreases the fairness of the final agreement[26]. Additionally, not having a strict rule of evidence in place can result in the presentation of irrelevant evidence that would complexity the process, therefore increasing the output of time and money. Furthermore, the privacy of the process is double-edged. It is perceived as an advantage for the parties, but it is also a disadvantage for the public. It could result in them not knowing information that could be harmful to them such as, conducting ADR in relation to the sale of expired or defective products. Lastly, the freedom enjoyed by third-party neutrals in regards to their commitment to the usage of previous cases creates a lack of precedents that don't aid in resolving later disputes of the same nature. In most ADR methods party agreements are binding between them as regular contracts and even in arbitration, res judicata is applied in the context of each particular dispute[27]. Finally, the greatest problem of ADR methods, notwithstanding binding arbitration, is the lack of enforcement of the final agreement when one party refuses to comply. The New York Convention for Arbitration has solved this problem. It has dictated the rules for award enforcement, which made arbitration a preferred destination for commercial disputes[28]. In turn, the evolution of arbitration with the added rules, expenses, formalities, and institutional governing have pushed it closer and closer to litigation and lessened the value of the aforementioned advantages of ADR.

B- Benefits and Challenges of ODR

a) Benefits of ODR

The previously mentioned advantages of ADR (cost and time-effective, conciliatory function, flexibility, and party autonomy) all apply to ODR. However, they are heightened and

[25] Andrew Tweeddale, Keren Tweeddale, Arbitration of Commercial Disputes, International and English Law and Practice, published by Oxford University Press, England, Oxford, 2005, pages 5,6
[26] Jacqueline Nolan-Haley, Alternative Dispute Resolution in a Nutshell, West Academic Publishing, 4th Edition, Minnesota, USA, 2013, page 59
[27] Manevy (Isabelle), OP. Cit. supra note 24, page 10
[28] United Nations Conference on International Commercial Arbitration, Convention on the Recognition and Enforcement of Foreign Arbitral Awards, United Nations, 1958, "The New-York Convention", Articles 2,5

complemented by additional advantages offered through the combination of ICT tools with ADR processes. In ODR there is a significant reduction in time and cost in comparison to judicial litigation and traditional ADR. This is the result of the instantaneous nature of communications through the internet and the development of high-quality video and audio systems. This is evident in cross-border disputes that involve several entities all over the world, where parties and arbitrators don't bear travel and accommodation expenses. All these logistics are bypassed through the advancement of ICT tools. Additionally, the process could start immediately rather than waiting to agree on details such as venue selection. All it takes is to set up a virtual meeting room with the involvement of a neutral third party from anywhere in the world, using a laptop or even a mobile phone. It is said that resolving a dispute online takes about 4 months, whereas obtaining a court decision through traditional ADR requires 18-36 months; with 35-60% fewer costs[29]. The importance of this advantage is seen in e-commerce disputes. Time-saving in these cases is priceless for both consumers and businesses since ODR enables early intervention, the prevention of dispute development, and the addressing of grievances before they turn into legitimate conflicts[30]. Furthermore, time spent on travel and other management operations in ADR and judicial systems is wasteful and could be emotionally and physically draining which would reflect badly in their decision making, so in ODR this time can be usefully utilized in researching, looking at data, preparing responses and strategies, and calming their emotions. Another benefit of ODR is that it provides better access to justice. This advantage relates to the previous two since it facilitates issues concerning travel and logistics for those who can't afford a trip physically and financially. Consequently, using ODR especially in disputes resulting from e-commerce, allows access to justice for everyone. Additionally, utilizing certain formats of ICT in ODR could remove the problems of bias resulting from ethnical, gender inequality, or racial differences that might not be directly evident while using audio systems or instant messaging platforms[31]. Moreover, foregoing face-to-face interactions could help weaker sides overcome the psychological intimidation of confrontation, as a result of power or economic imbalances[32]. Furthermore, the internet offers a neutral venue in cyberspace for disputants where no one has an advantage because

[29] Karim Benyekhlef, Fabien Gelinas, Online Dispute Resolution, Lex Electronica, Volume 10, No. 2, 2005, page 86, found at https://www.lex-electronica.org/files/sites/103/10-2_benyekhlef-gelinas.pdf visitation date 12/5/2021
[30] Rule (Colin), OP. Cit. supra note 9, page 77
[31] Ibid, page 68
[32] Hörnle (Julia), OP. Cit. supra note 12, pages 89,90

of his/her actual place of living. Thus, the stronger or weaker party can't strategically exploit their actual "home court advantage" which puts them on equal footing[33].

The aforementioned ODR advantages all serve the purpose of convenience. Through the integration of technology with ADR, the convenience offered to the parties and the neutral third have significantly increased. Thus, resulting in better outcomes that satisfy the pursuit of fairness and justice, and conform to the way business and disputes arise in the virtual world. For example, in online commerce, it is only natural to handle such cases online. The origination and entirety of the relationship that is related to the parties have taken place virtually, therefore resolving their disputes should also happen in the same medium. From the perspective of online consumers and business owners who purely conduct their business online, it is weird for them to meet face to face to resolve their virtual issues. Moreover, the convenience provided by cyberspace can impact how neutral third parties moderate the dispute, where aggression portrayed by disputants can't exceed verbal comments, which could be easily defused, and allows the parties to focus on achieving a resolution rather than perceiving other parties as enemies. Also, recording and digitally archiving the process could aid disputing and third-party neutrals in reaching better outcomes and making well-informed decisions by revisiting them. An added benefit of the recording system is that it provides irrefutable grounds for accountability issues since it can be utilized to check on the behavior of the neutrals, disputing parties, and their representatives[34]. Furthermore, the convenience of ODR has become extremely important and useful during COVID-19. Strict regulations concerning travel, nationwide lockdowns, curfews, and lack of interactions would have completely crippled the judicial and extra-judicial systems if it weren't for ICT and the convenience it offered them. Finally, the flexibility trait of ADR is also taken to new heights in ODR. It could offer more flexibility in choosing the law that applies to the process, the neutral third, and other aspects of the dispute that would be easier since the obstacles of place, time, and cost are removed. Additionally, through ICT used in ODR, parties could convey their ideas better through visual and audio-visual presentations with explanations that would allow for real-time fact-checking and verification of the information presented. Moreover, ICT could increase the flexibility of the process by offering advanced tools for arbitrators, which would result in better

[33] Victorio M. (Richard), OP. Cit. supra note 14, page 14,15

[34] Fangfei Faye Wang, Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective, Chandos Series on Publishing, 1st Edition, Oxford England, 2009, page 29

case management. However, as it is with ADR, the traits that give ODR its advantages also create disadvantages, rendering them as double-edged swords.

It is noteworthy to mention, that these advantages and the upcoming disadvantages are being addressed in their general context in relation to ODR as a whole. However, some advantages of online arbitration can be disadvantages for online mediation and negotiation and vice versa.

b) The Challenges of ODR

Having an extra-judicial system of dispute resolution operating entirely in cyberspace is bound to create a new set of challenges that accommodate the nature of the digital world. These obstacles can be due to the practicalities of using ICT, the authenticity of involved parties, data security and confidentiality concerns, and challenges that accompany the enforcement of online decisions or awards. The segment will briefly discuss the first 4 challenges, leaving enforcement mechanisms to the following section.

Firstly, the practical challenges of ODR could be a result of the illiteracy of participants concerning the utilization of ICT tools. This particular challenge has significantly decreased, since computers, smartphones, and other ICT tools have become widely available and accessible for the majority of people[35]. However, some countries still lack the proper infrastructure to provide a smooth and secure online dispute resolution experience, in addition to the vast differences in internet speed[36]. More importantly, having access doesn't necessarily mean operational knowledge. Some parties who have access to these tools may have difficulties operating them, especially those who aren't willing to or can't put in the time and effort to learn how they function. Moreover, participating in ODR isn't just about having access, average knowledge of use, and good internet. It requires users (participants, ODR practitioners) to have certain skills. As mentioned by Kathleen Paisley in a webinar on data protection and cybersecurity, being a successful arbitrator or mediator demands that practitioners be multi-specialized, well-versed, and

[35] "As of January 2021, there were 4.66 billion active internet users worldwide - 59.5 percent of the global population. Of this total, 92.6 percent (4.32 billion) accessed the internet via mobile devices." Found at https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20January%202021%20there,the%20internet%20via%20mobile%20devices visitation date 18/4/2021

[36] For example, most third-world countries don't have an adequate internet connection. This applies to Lebanon, which in 2019 ranked 167th globally in worldwide broadband speed. Found at https://economics.creditlibanais.com/Article/209231 visitation date 18/4/2021

always on the lookout for new developments in several fields (i.e., economy, technology, cybersecurity, etc.)[37]. For some participants or practitioners, this could be intimidating especially in regards to the use of technology that is constantly changing and evolving at an unprecedented speed. To overcome these difficulties, one might hire experts to train them or operate on their behalf, but this will result in the accumulation of extra costs, before even starting with the actual matter at hand[38]. However, there is a rebuttal for such claims. Nowadays an increasing number of people are familiar with the proper use of these platforms, and that such arguments may be more accurate in disputes that occur offline because parties that possess adequate knowledge to conduct online transactions that result in disputes can also utilize that knowledge in ODR. Another practical drawback is based on the lack of face-to-face or physical interaction, especially when the majority of the process is done through messaging platforms. Through these mediums, it is difficult to understand the actual content of the message, the tone, or the underlying meaning behind it, which causes misunderstandings to happen and the constant need for clarifications. Additionally, body language is so important in some forms of extrajudicial dispute resolution, since it offers insight into a deeper level of an understanding of the parties and their intentions. Although modern technologies have provided methods of interaction that simulate real-life contact, yet natural face-to-face confrontations remain different. For example, mediation or negotiation are mainly built around trust. It all comes down to bridging different opinions through education methods, persuasion, reflection, and reexamination. For this trust to happen it needs to be felt, and not done through a written exchange of messages or even virtual meetings. Moreover, recording and archiving communication with the ability for parties to constantly visit them may cause additional problems. This could occur in cases where parties constantly revisit instances of altercations and get too emotionally attached to them. Thus, it could increase hostility, and may not allow parties to move onward with finding a solution[39].

Secondly, the nature of ODR brings about several concerns in regards to the authenticity of identities and documents, data security, and confidentiality. In regards to the authenticity of people and documents, this argument seems outdated now. Videoconferencing technologies have

[37] CIArb Singapore "Cybersecurity and Data Protection Webinar", Virtual seminar held on Zoom, November 24, 2020
[38] Victorio M. (Richard), OP. Cit. supra note 14, pages 20,21
[39] Rule (Colin), OP. Cit. supra note 9, pages 80,81

developed tremendously to allow parties to know exactly the person they are dealing with. Additionally, there are verification tools that would allow for the authentication of documents and signatures[40]. Moreover, as said in the advantages of ODR, every piece of information or document presented could be instantaneously fact-checked. The primary concern with ODR is issues of confidentiality and data security. As previously mentioned, confidentiality is the essence of extra-judicial dispute resolution processes, and it's the main attraction for parties to engage in them rather than judicial litigation. Information shared during any ODR process is usually retained and stored in digital copies, and transmitted across digital channels from one place to another. Thus, information concerning the process faces a risk of being exposed through cyber-intrusions, attacks, or wrongful processing and misuse. It is noteworthy to mention that the internet inherently works in a way that allows it to create several copies of documents when data is being transferred[41]. Additionally, information retention online can cause significant damage to peoples' reputation or safety, since emails or any other forms of online documents can always be retrieved regardless of when it was made or where it was stored. Moreover, in cyberspace, there is always a risk of message interception or temperance from the parties involved or unknown third parties. In this sense, data can't be absolutely safe, forgotten, or permanently deleted. Therefore, users need to be extra careful in regards to their online activities. Accordingly, parties will be reluctant to share confidential information if they aren't provided with guarantees of a suitable and safe environment for such processes.

Another aspect of concern is cybersecurity. There is a myriad of ways through which information and data in cyberspace could be exposed and it significantly hurts the value and reliability of ODR. One could argue that no medium, whether actual or virtual, is safe from violations and breaches, and that the most anyone could do is set up protective shields and barriers to limit or mitigate the risk of falling victim to malicious acts. However, ODR may likely have a negative impact on data protection and privacy through the consideration that shifting to online justice will generate a huge increase in online data, which in turn increases processing, controlling, cybercrime, and the dependency on artificial intelligence. In other words, the increase in the amount of data in cyberspace will be proportional to the increase of misuses and violations. For this reason, the need

[40] Manevy (Isabelle), OP. Cit. supra note 24, page 31

[41] Esther van den Heuvel, Online Dispute Resolution as a Solution to Cross-Border E-Disputes: An Introduction to ODR, 1997, page 15, found at http://www.oecd.org/internet/consumer/1878940.pdf visitation date 19/4/2021

for collective counterbalancing acts is necessary for the domains of data protection and cybersecurity[42]. Fortunately, the international community has become increasingly aware of cyber-threats and is working on providing a reliable and safe cyberenvironment. Additionally, as seen through the discussion of the GDPR, the European Union has created a borderless regulation that can match the borderless nature of the internet and the nature of the crimes and data misuses that came along with it.

Despite all the benefits that accompany the use of ICT in dispute resolution, the use of these mechanisms isn't without risks. This will be extensively addressed in the next chapter which discusses cybercrimes, their perpetrators, and their impact on the real world. When committed, these aggravations could cripple ODR and expose parties' trade secrets, valuable information, ruin reputations, negatively impact and expose information of third parties, and damage the integrity of the dispute resolution institution as a whole. Thus, the maximum utilization of ICT tools can be challenging, especially when factoring in the risks that accompany it. Hence, giving rise to the argument that ICT tools should be only used in moderation and as facilitators of the process that only contribute to the extent of the positive evolution of traditional ADR[43]. In contrast, it could be argued that the appropriate cybersecurity measures and data protection regulations, coupled with the awareness of the involved parties could greatly mitigate those risks.

To conclude this section, it is clear that in ODR every advantage or benefit provided by one of its traits is accompanied by a disadvantage or downside. This could be attributed to the novelty of ODR, the constant change and modification of ICT tools, and the attachment to traditional ways of dealing with conflicts. Moreover, the difference in global capabilities, access, and awareness, disrupts the potential growth of online processes and limits the ability to reach worldwide solutions. It remains to be seen how ODR has impacted enforcement mechanisms, especially in binding arbitration, and the potential impact of future technologies on judicial and extra-judicial systems.

---

[42] European Committee on Legal Co-operation (CDCJ), Technical Study on Online Dispute Resolution Mechanisms, CDCJ (2018) 5, Strasbourg, August 1, 2018, pages 60,61, found at https://rm.coe.int/cdcj-technical-study-on-online-dispute-resolution-mechanisms/16809f0079 visitation date 18/4/2021

[43] Richard Hill, Online Arbitration: issues and solutions, Article, Published in Arbitration International, Volume 15, Issue 2, June 1, 1999, pp. 199-207, page used 199, found at http://www.umass.edu/dispute/hill.htm visitation date 25/4/2021

SUB-CHAPTER 2: The Significance of IT Developments in Extra Judicial and Judicial Systems

The development, use, and dependency on IT tools are constantly increasing. Accordingly, it has and will continue to have a profound impact on the functionalities of extra-judicial and judicial processes. This Sub-Chapter will shed light on International Efforts in adopting ODR practices due to COVID-19, and some of the issues caused by IT integration in ODR, especially online binding arbitration, in regards to enforcement, validity, consent, and the applicable law (Section 1). Whereas, (Section 2) will offer a brief insight into the impact of future developments on these processes such as AI.

SECTION 1: The Shift Towards ODR and its Practical Adoption

As discussed, the shift towards ODR has been a work in progress for a couple of decades now. However, recent developments have forced an international acceleration in adopting virtual means of communications that proved to be crucial for business continuity. For this reason, (Sub-Section 1) will showcase how COVID-19 elicited an international uprise concerning the use and enforcement of ODR. Whereas, (Sub-Section 2) will provide some noteworthy issues to consider while applying online arbitration.

Sub-Section 1: International Efforts in Migrating to ODR due to COVID-19

At the time of writing, almost two years of the COVID-19 pandemic have passed. One of its biggest impacts was on business and consumer transactions. The strict lockdown regulations have forced several sectors all over the world to shut down, cease their operations, or compelled them to migrate to online methods or to “work from home”. When the aforementioned protocol was drafted in 2018, it was preparing for the imminent shift and the increased dependency on information technology in arbitration. However, the unforeseen COVID-19 pandemic hastened the transition and reliance on digital platforms needed to conduct arbitral proceedings. As a result, parties are exclusively communicating online, filing and exchanging documents electronically, storing files online, carrying out hearings via telephone or videoconference, or using virtual rooms for full hearings. The flexibility, readiness, and pre-established use of information technology and its tool have been introduced to the arbitral process which allowed for a relatively smooth transition. However, concerns related to cybersecurity have increased, especially that parties and

the tribunal are bound by the necessity of the situation to use technologies that may be unfamiliar to them, and use unprotected networks or home devices, rather than the managed and well-secured IT assets in a relatively safe and controlled work-place environment. Thus, the "weak link" represented by humans and their personal devices has gotten weaker, especially since hackers and other malicious actors are using COVID-19 related texts, emails, and links as "bait" to launch cyber-attacks on new and vulnerable remote working infrastructure. Hence increasing the relevancy of the baseline information security measures addressed by the ICCA- New York Bar-CPR Cybersecurity Protocol which will be examined in the final chapter. Accordingly, the following segment will highlight some institutional and organizational responses and actions in dealing with the current situation[44].

A- Concerning Staff, Offices, and Pending Cases[45]

The majority of institutions have closed their offices and moved to remote working arrangements, for all or a majority of employees. Institutions like the Financial Industry Regulatory Authority (FINRA), the Arbitration Institute of the Stockholm Chamber of Commerce (SCC), and the Vienna International Arbitral Centre (VIAC) digitalized certain features of their case management procedures using new platforms and portals before the start of the pandemic, so they're seeking to utilize these means to conduct their business as close to normal as possible. Organizations such as the Judicial Arbitration and Mediation Services, Inc (JAMS) prepared some precautionary steps that follow governmental protocols concerning cleaning routines, using plexiglass screens, social distancing, and limiting the number of cases heard at the same time and place, which will see several institutions adhering to. Additionally, the International Centre for Dispute Resolution (ICDR) announced that due to COVID-19, it will continue to provide virtual hearings. Moreover, concerning pending cases, almost every institution has put in place business continuity and contingency plans. These plans will facilitate and ensure that pending cases are

[44] Information previewed in this segment about specific key institutional and organizational initiatives- except for the Seoul Protocol- can be found in a table format at https://hsfnotes.com/arbitration/wp-content/uploads/sites/4/2020/06/COVID-19-Responses-of-Institutions-and-Organisations-11-June-2020-HSF-Arbitration-Notes.pdf visitation date 10/1/2021

dealt with remotely or through limited in-office support. For example, the SCC is allowing parties with pending cases initiated before September 2019 to move case data to the SCC Platform.

B- General Case Administration

The majority of institutions have allowed requests/notices of arbitration to be filed through email for the duration of the pandemic, while others such as the International Centre for Settlement of Investment Disputes (ICSID), the Swiss Chambers' Arbitration Institution (SCAI), and the German Arbitration Institute (DIS) have continued to accept hard copies using ad hoc arrangements. Additionally, the use of USB by the Cairo Regional Centre for International Commercial Arbitration (CRCICA) and telefax by (DIS) were also admitted.

C- Communications

The overwhelming majority of organizations have migrated to digital means of communications (electronic or telephonic), and only a select few still permit documents or communications to be sent through post or via couriers. Institutions such as the DIS and SCC that had heavily integrated IT in their proceedings before the pandemic swiftly and easily conformed to the new requirements. Moreover, the SCC made its digital platform in partnership with Thomson Reuters available and free of charge for ad-hoc arbitrations commenced globally during the pandemic.

D- Hearings (Virtual meetings and hearings)

Given that almost all in-person hearings have been canceled and rescheduled, with others being conducted virtually. The use or proposition of use of commercially available services such as Skype, Facetime, Zoom, Microsoft Teams, and Facetime have been adopted by several organizations such as the ICC, SCC, JAMS, IDRC, and LMAA, while other organizations are promoting the use of bespoke services. For example, there is the ICSID video conferencing platform and the Singapore International Arbitration Centre's (SIAC) collaboration with Maxwell Chambers' Virtual ADR service. Accordingly, as mentioned, the use of commercially available platforms has many downsides, but desperate times call for desperate measures, especially in

arbitral cases where time is of the essence and the availability and accessibility of bespoke platforms is a scarcity[46].

In this context, it's noteworthy to shed light on the Seoul Protocol on Video Conferencing in International Arbitration. It was developed in 2018, during a discussion of videoconferencing at the 7th Asia Pacific ADR Conference in Seoul, South Korea, and largely concluded before the pandemic. The initial purpose of the protocol was for complex arbitrations that used high-end technologies, but it provides a useful guideline for those attempting to self-manage small-scale arbitrations using online platforms. This protocol offers practical guidance that can serve similar roles as the UNICITRAL Notes on Organizing Arbitral Proceedings, while primarily focusing on witness testimony presentation through videoconferencing. Additionally, the guidelines of the Seoul protocol have recognized the risks associated with the use of online technology in a process that is based on confidentiality. Therefore, it aims to familiarize and help participants address these persisting issues[47].

Furthermore, in an attempt to prepare for the future, the ICDR is anticipating the establishment of "semi-virtual hearings" or "global hybrid hearings" where only the arbitrators and the counsel are at the center and participants use videoconference technologies. This could be beneficial in mitigating costs and travel expenses, as well as travel restrictions. However, getting all the different human and technical elements of this operation to work together in conjunction with perfect alignment and efficiency will prove to be cumbersome and difficult, especially with the difference in technological availability, capability, and accessibility in international matters involving parties from second or third world countries. Furthermore, on a practical level, it may be difficult in some cases for parties to jointly agree on virtual hearings, for one party may insist on having a virtual hearing while the other would want a normal hearing[48].

---

[46] Information previewed from (A) to (D) are based on: Herbert Smith Freehills Arbitration Notes, Update [6]: "Necessity is the Mother of Invention": Covid-19 Dramatically Accelerates Digitalization of Arbitration Processes, 12/6/2020 found at https://hsfnotes.com/arbitration/2020/06/12/update-6-necessity-is-the-mother-of-invention-covid-19-dramatically-accelerates-digitalisation-of-arbitration-processes/ visitation date 10/1/2021

[47] Tony Cole, The Seoul Protocol on Videoconferencing and the Coronavirus (COVID-19) Pandemic, Article, published May 14, 2020, found at https://www.lexology.com/library/detail.aspx?g=577b26b4-5372-4bc4-afba-ad72e60a94ba visitation date 10/1/2020; see also http://www.sidrc.org/static_root/userUpload/data/[FINAL]%20Seoul%20Protocol%20on%20Video%20Conference%20in%20International%20Arbitration.pdf for the actual protocol visitation date 10/1/2020

[48] Herbert Smith Freehills Arbitration Notes, OP. Cit. supra note 46

Last but not least, the effectiveness of these new methods will be determined based on the willingness, cooperative mindset, and ability of tribunals, practitioners, and parties to conform with and embrace what these technologies offer.

Sub-Section 2: Noteworthy Issues to Consider in Online Arbitration

A- Validity of Online Arbitral Agreement

In traditional arbitration, the validity of the agreement, recognition, and enforcement of foreign arbitral awards are mainly guaranteed by the "New York Convention". However, does this coverage extend to the validity of online arbitral agreements? Under Article 2 of the "New York Convention", a valid arbitral agreement should be concluded in writing[49]. This stipulation under the New York Convention in 1958, didn't and couldn't have expressly included online means of concluding an agreement, since the New York Convention was established before the existence of ICT tools. However, the UNCITRAL Model Law on International Commercial Arbitration" in 1985 had a broader description of "agreement in writing" that covers all means of telecommunications and uses the concept of "data messages" such as telex, telegram, telecopy, etc., but the information contained therein should be accessible and usable for subsequent reference[50]. This issue could be bypassed by making a hard copy of the agreement, but it would mean losing the plot of conducting the entire process online. Another solution is to broadly interpret the New York Convention based on the UNCITRAL Model Law, as to include emails and other means of ICT since they are an updated version of telex, telegram, and other means recognized by UNCITRAL. Additionally, the EU and several other laws support this notion. For example, the EU "Directive on Electronic Commerce" accepts the conclusion of contracts by

[49] The New York Convention, OP. Cit. supra note 28, Article 2 which stipulates: "Each Contracting State shall recognize an agreement in writing under which the parties undertake to submit to arbitration all or any differences which have arisen or which may arise between them in respect of a defined legal relationship, whether contractual or not, concerning a subject matter capable of settlement by arbitration" "The term 'agreement in writing' shall include an arbitral clause in a contract or an arbitration agreement, signed by the parties or contained in an exchange of letters or telegrams".

[50] UNCITRAL Model Law on International Commercial Arbitration, 1985, Article 7, found at https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-54671_ebook.pdf

electronic means[51], and the UK "Arbitration Act" of 1996 which accepts in written form anything being recorded by any means[52].

B- Consent in Electronic Arbitration Contracts

Expressing consent online is another issue with ODR methods. As mentioned, ICT tools can replace the traditional ways of obtaining consent in a secure and guaranteed manner. Usually, consent is ensured through signatures. Accordingly, the New York Convention expressly requires the arbitration agreement to be signed by the parties. This requirement is met through the utilization of electronic signatures. The use of digital signatures and authentications are backed by encryption technology, which is commonly applied in electronic commercial transactions to guarantee online business security[53]. The digitalization of signatures is backed by several international initiatives that are trying to create a framework that promotes and harmonizes the use of electronic authentications globally in e-commerce. For example, the "UNCITRAL Model Law on Electronic Signatures" adopted on July 5th, 2001; the "General Usage for International Digitally Ensured Commerce", the "e-Terms", and the "Guide to Electronic Contracting" all adopted by the International Chamber of Commerce (ICC), serve the purpose of creating a basis for the use of digital signatures in international commercial transactions.

C- Issues Regarding the Place or Seat of Arbitration

The importance surrounding the place or seat of arbitration has to do with its direct influence on other aspects of the process. Seat designation in a certain legal jurisdiction may impact the nationality of the award, the courts responsible for its recognition, enforcement, and supervision. Accordingly, how can these principles be applied in the context of an online format of dispute resolution which takes place in a virtual world without physical boundaries? In order to avoid what is known as "floating arbitration" which leads to "Floating awards" causing several consequences, the principle of party autonomy should be applied. Through this principle, parties can choose the

[51] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Recital 17, found at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031
[52] UK Arbitration Act of 1996, Section 5, Found at https://www.legislation.gov.uk/ukpga/1996/23/data.pdf
[53] Wang F. (Fangfei), OP. Cit. supra note 34, pages 18-23

seat of arbitration and proceedings can be concluded in a country other than that of the place of arbitration, without causing them to change the seat of arbitration[54]. This notion is reinforced by the delocalization theory, which stipulates that arbitration should be detached from the place of arbitration[55]. Furthermore, online arbitration shouldn't be considered in terms of traditional arbitration. In other words, it is not suitable to apply the laws and conditions of the physical world or the virtual world. Thus, the seat in online arbitration can't be defined as the place of the procedure or the place where the arbitrator is located, or where the award was made. It should be understood as a legal criterion and defined based on a "seat designation agreement" determined by the parties or arbitrators or ODR providers. Hence, the seat of arbitration is a matter of designation and independent from any physical location. The idea that the place and seat of arbitration are designated by the parties based on their agreement is supported by the UNCITRAL Model Law Article 20[56], ICC Arbitration rules Article 18[57], and national laws such as in France[58].

D- Issues Regarding the Applicable Law

Choosing the applicable law in online arbitration influences which law will govern the arbitral agreement, the procedural issues, and the substantive issues. Similar to the previous point, the principle of party autonomy would solve the question of applicable law, for it allows the parties to determine the applicable law. Accordingly, parties can avoid jurisdictional problems and choice of law issues. Thus, parties may agree on using the substantive law through national law, specific

[54] Ibid, page 89

[55] Dejan Janićijević, Delocalization of International Commercial Arbitration, Article, published in Facta Universitatis, Law and Politics Volume.3, Number 1, 2005, pp. 63-71, page used 64, found at http://facta.junis.ni.ac.rs/lap/lap2005/lap2005-07.pdf visitation date 19/4/2021

[56] UNCITRAL Model Law, OP. Cit. supra note 49, Article 20

[57] International Chamber of Commerce (ICC), 2021 Arbitration Rules, Article 17, found at https://iccwbo.org/content/uploads/sites/3/2020/12/icc-2021-arbitration-rules-2014-mediation-rules-english-version.pdf

[58] The French Cour de cassation has adopted the same stand and states that "the seat of arbitration is a purely legal concept, which has important consequences, notably concerning the jurisdiction of national courts regarding appeals for annulment; (the choice of the seat) depends on the will of the parties, it is not a physical concept which depends on the place where the hearings took place or the place where the award was signs, places which can vary according to the fancy and clumsiness of arbitrators. See Cass, 1ère civ, 28 October 1997, Société Procédés de Préfabrication pour le béton c/ Libye, Revue de l'arbitrage 1998, p.399-407

state, or international rules such as the "lex mercatoria" or its online equivalent "lex informatica"[59] to govern their proceedings.

E- Enforcement of Awards

Party compliance and enforcement of awards in ODR cause major concerns. This issue is magnified by the borderless nature of disputes resulting from electronic contracts. In this sense, it is important to distinguish between different procedures of binding and non-binding ODR methods. In the first type, enforcement and compliance are generally easier because of the binding nature of the process which compels parties to comply. Additionally, the utilization of international treaties in arbitration makes it easier to enforce and comply with disputes having international elements and cross-border transactions; it only needs an initiation of an exequatur by the winning party. However, it is much more difficult to guarantee compliance and enforcement in non-binding processes, especially when dealing with cross-border disputes. This issue could be partially solved with the inclusion of a binding settlement agreement, which renders the outcome binding as a normal contract. Nonetheless, this doesn't present an effective solution, for the absence of voluntary compliance by the parties will result in them referring to judicial courts to obtain enforcement decisions. Thus, going back down the same route of judicial litigation they wanted to avoid in the first place since the absence of voluntary compliance will require the winning party to refer the case to court and start a new court action. The same process applies to enforcement proceedings and binding awards, which will generally cost more time and money, especially in cross-border disputes. Hence, defeating the original purpose of choosing ODR. For this reason, the lack of enforcement mechanisms in non-binding ODR is considered to be one of its most important drawbacks

Under the "New-York Convention", the UNCITRAL "Model Law on International Commercial Arbitration", and other country laws, arbitral awards must be written and signed by arbitrators and

[59] Lex Informatica is defined as: "the body of transnational rules of law and trade usages applicable to cross-border e-business transactions, created by and for the participants in cross-border e-business and applied by arbitrators to settle disputes on the basis of the intention of the parties and taking into account the rapid evolution in the state of the art of e-business" See Antonis Patrikios, Resolution of Cross-border E-business Disputes by Arbitration Tribunals on the Basis of Transnational Substantive Rules of Law and E-business Usages: The Emergence of the Lex Informatica, 21st Bileta Conference, Malta, April 2006, pages 15,16, found at https://www.bileta.org.uk/wp-content/uploads/The-Emergence-of-the-Lex-Informatica.pdf visitation date 30/4/2021

the parties. This issue has caused controversy as to whether online awards in an electronic form with digital signatures are valid under the previous rules. This issue can be avoided by simply making a certified hard copy of the award and signing it traditionally. Another solution that has been adopted by the international community is to broadly interpret the "New York Convention" under the functional equivalency of online awards and digital signatures. The same concern arises in regards to the enforcement of the award. Under the "New-York Convention", the recognition and enforcement of the award require its presentation via "a duly authenticated original of the award or a duly certified copy"[60]. Therefore, this creates another concern regarding digital awards and signatures. Hence, resorting to the same solutions presented for the first concern. Hoverer, there should be a more permanent solution. This convention entered into force in 1958, so it couldn't have possibly foreseen what would have transpired in regards to digitalization and the nature of modern contracts. Thus, rather than constantly interpreting and broadening its scope of application with the emergence of new technologies, it would be better to amend the Convention to better suit modern times.

It is important to mention that the aforementioned issues discussed in this segment are just a small portion of the questions that ICT integration has brought to extra-judicial proceedings. There are several more matters and debates surrounding binding and non-binding ODR processes. However, the purpose of this segment was to shed light on how online proceedings that occur in cyberspace require a different approach and perspective in regards to their initiation and conclusion. Accordingly, binding online arbitration has provided this opportunity, since its traditional equivalent is governed by concrete laws and international conventions, which added a legal context to the comparisons drawn between the traditional and online methods. In turn, other non-binding dispute resolution mechanisms lacked this legal and comparative aspect since they are mainly dependent on consensual agreements.

Lastly, it is incumbent for the purpose of this thesis that we touch upon the most recent IT developments and the potential impact they have on the extra-judicial and judicial systems.

[60] The New-York Convention, OP. Cit. supra note 28, Article 5

SECTION 2: The Impact of Artificial Intelligence on Litigation

Artificial intelligence, robot-judges, blockchain systems, and cryptocurrencies are some of the most intriguing representations of digitalization. They have the potential to change the future to an unrecognizable extent. However, these technologies are still in their infancy, and it would take several iterations for them to reach a level that would replace traditional norms. Nonetheless, the fear of the unknown has sparked several debates among scholars and others, especially due to the growing concern that AI would replace humans in judicial and extra-judicial processes. Accordingly, an insight into this debate would help enrich the context of this thesis and provide a sneak peek into what the future might hold for us.

A- Defining AI

The main difference between AI and other IT tools is their ability to constantly learn and evolve when they are utilized. AI could be split into two main types: rule-based learning and machine learning. The first category is used for static and slow-based scenarios, while in the latter AI can identify patterns and changes its algorithm based on pre-existing data and user feedback[61]. To go even deeper, a subset of machine learning is the deep learning model (artificial neural networks), which mimics the structure of the brain. It identifies aspects without human interference through learning from heavy volumes of pre-existing data. The potential of this subset is recognized through its work on unstructured data. Thus, the combination of deep learning and natural language processing allows AI to perform and comprehensibly present tasks that require human intelligence[62]. Moreover, another key subset in the machine learning model is predictive analytics, which determines a course of action, and derives possible outcomes and consequences of such decisions[63].

---

[61] Aditya Singh Chauhan, Future of AI in Arbitration: The Fine Line Between Fiction and Reality, Article, Published in Kluwer Arbitration Blog, September 26, 2020, found at http://arbitrationblog.kluwerarbitration.com/2020/09/26/future-of-ai-in-arbitration-the-fine-line-between-fiction-and-reality/ visitation date 19/4/2021

[62] Jake Frankenfield, Artificial Neural Network, e-Article, published in Investopedia, updated August 28,2020, found at https://www.investopedia.com/terms/a/artificial-neural-networks-ann.asp#:~:text=An%20artificial%20neural%20network%20(ANN)%20is%20the%20piece%20of%20a,by%20human%20or%20statistical%20standards visitation date 19/5/2021

[63] Jake Frankenfield, Predictive Modeling, e-Article, published in Investopedia, update June 27, 2019, found at https://www.investopedia.com/terms/p/predictive-modeling.asp visitation date 19/4/2021

B- Employing AI in International Arbitration

The use of AI at two of its initial levels such as for natural language processing (i.e., translation, classification of clustering, information extraction) and expert systems can be valuable to arbitration. Accordingly, AI could help analyze data from awards and arbitrator intelligence questionnaires[64] to assess an arbitrator's inclinations through its decision-making at different stages of processes in the past. Additionally, AI could prove very helpful through tracing the relevant experience of arbitrators on different types of matters and disputes. Thus, the combination of these two systems would provide a credible source of arbitrator selection. Hence, filtering out arbitrators based on an AI system through computing data based on expertise, the subject matter of the dispute, success rate, and other criteria could improve the quality of the whole process, from selection until resolution. Furthermore, the use of AI's lower-level tools for translations and data mining to assess, separate, organize, and summarize clusters of data, would be hugely beneficial for the process, especially since it decreases time and cost, thus increasing efficiency and user satisfaction[65].

On the flip side, the excessive interference of AI with the adjudicatory process through its decision-making capacity can become problematic, especially to those that could be possibly replaced by such technologies (i.e., paralegals, associates mainly, followed by arbitrators, judges). Whether this assumption is valid or not will be seen with time, but it remains a thought worth entertaining.

Based on the accounts of several people among which are Janet Fuhrer and Art Cockfield about the question of whether they think AI will terminate jobs for lawyers, create new ones, or both. Janet Fuhrer thought that AI has the potential to cause both. AI could easily replace students, junior lawyers, and paralegals in the jobs they do. However, she thinks that there are still many opportunities for them, even with technology, to provide services. Whereas, Art Cockfield based his response on his own personal experience of "drudge work" and several years of doing due

[64] See https://arbitratorintelligence.com/AIQ-English.pdf

[65] Falco Kreis, Markus Kaulartz, Smart Contracts and Dispute Resolution – A Chance to Raise Efficiency? ASA Bulletin, Volume 37, Issue 2, June 2019, pages 337, 350

diligence. He concluded that many jobs, especially in big law, could potentially disappear because of AI[66].

Meanwhile, in China, Dr. Anyu Lee who is a strong advocate of robot-judges described the potential of AI in resolving disputes in an ODR forum in October 2019. He believes that the small value cross-border e-disputes that have proliferated with global digitalization which are burdensome to resolve and require many resources could be resolved easily soon with AI. Accordingly, he concluded that robot-judges, robot-arbitrators and robot-mediators are the way forward in solving such small value disputes, and enforcement of their resolutions can be achieved through a social credit system. Moreover, Dr. Lee asserts the idea that advanced robot-judges can render correct and consistent decisions because of their ability to speak multiple languages, analyze large sets of court related data, and know the laws of different jurisdictions. However, the question of whether a robot-judge of any kind can be fair is still far-fetched, for the concept of fair justice is deeply intertwined with human ethics. Thus, for a robot-judge in any capacity to be fair, it should be able to ask ethical questions and have ethical principles[67].

First of all, at this time, AI depends on large data sets and user feedback. In the context of arbitration, most documents are confidential and exist in relatively smaller data sets when compared with the judicial system. Additionally, the myriad of diverse laws, practice areas, and variables that go into a single process can limit the ability of training and testing. An alternative would be to establish a localized program where AI is used, tested, and fed information of a specific legal system, thus controlling certain variables in the process. However, the nature of disputes has become increasingly borderless with a complex integration of different laws, procedures, and fields. Moreover, the individual assessment and case-by-case resolutions, coupled with the lack of precedents in arbitration decreases the effectiveness of AI in this domain[68].

Another layer of the question of whether AI will replace human arbitrators is approached from the cognitive and emotional superiority of humans that of which is absent in AI. Additionally, it

---

[66] How will artificial intelligence affect the legal profession in the next decade, Debate under Queen's Law Reports, November 3, 2015, found at https://law.queensu.ca/news/how-will-artificial-intelligence-affect-the-legal-profession-in-the-next-decade visitation date 19/5/2021

[67] Zbynek Loebl, Can a robojudge be fair, Article, Published in Kluwer Arbitration Blog, December 16, 2019, found at http://arbitrationblog.kluwerarbitration.com/2019/12/16/can-a-robojudge-be-fair/ visitation date 19/5/2021

[68] Chauhan S. (Aditya), OP. Cit. supra note 61

should be understood that the current state of laws revolves around natural persons. Moreover, AI still lacks the capacity to provide clarifications and award reasonings as per party requests. It could provide binary and objective analysis that would amount to probabilistic inference at most[69]. Furthermore, some assert that AI can be absolutely independent and impartial, since it filters all emotions, biases, and is based on objective data and statistics. However, data bias is worse than arbitrator bias, since the latter can be deduced and recognized thus challenging the arbitrator's inclinations. This could lead to establishing grounds for the liability and accountability of arbitrators, whereas the same can't be said in regards to AI, for it is not possible to challenge an AI's bias and hold it accountable. Also, if most arbitrators whose data has been collected, computed, and analyzed have expressed intangible bias towards disputants in regards to their ethnicity, race, sex, or social standards. These biases will be also present in the AI, resulting in faulty and impartial machines[70].

Whether or not AI will replace humans soon, there is no denying that we are in the midst of a new tipping point in human history. The magnitude of which is yet to be fully understood or conceived by the human mind. The same can be said about the monetary system which had gone (from gold to paper currency) and might once again go (from paper currency to cryptocurrency) through unimaginable changes. The shift from analog to digital has been ongoing for quite some time now, and we are now on the verge of starting a new shift. Twenty years ago, who would've thought that mobile phones, especially smartphones, are going to take over every aspect of our lives. They started off as simple tools and developed into facilitators and then became extensions of ourselves. Now, however, we have become so integrated and deeply rooted in them that the separability that once existed has almost vanished. A smartphone has more data and knowledge about a person; their family, friends, and enemies; likes and dislikes, than the person himself. It can even be said that smartphones can dictate a user's behavior, and consciously or subconsciously manipulate their decisions, thus dictating their future. In other words, the conceived notion about robot-judges or any representation of AI to be physical entities with metal-like bodies that will

[69] Maxi Scherer, Artificial Intelligence and Legal Decision- Making: The Wide Open? A Study Examining International Arbitration, Article, Published in the Journal of International Arbitration, Volume 36, Number 5, 2019, pp. 539-574, pages used 540, 556-567, found at https://3rdsifocc.tpi.sg/assets/documents/SCHERER%20Artificial%20Intelligence%20and%20Legal%20Decision-Making[7].pdf visitation date 5/1/2021

[70] Chauhan S. (Aditya), OP. Cit. supra note 61

suddenly creep up on society and take their jobs isn't all that accurate. The more likely scenario is that the already established integration between AI and humans, which we have been so reliant on for the past two decades, extends even further with exponentially better computational power, efficiency, speed, and reliability. In simpler terms, rather than having to access Google or any other website from a smartphone, people may have the ability to do so with a chip inside their brains. This concept is a work in progress and was introduced by Elon Musk through what is known as "Neuralink"[71]. Although it still needs several iterations to reach this level and become commercially available, it seems like the most probable outcome.

In conclusion, although the digitalization of ADR and especially the arbitral process has its perks, all those institutional and organizational initiatives, platforms, and protocols could be detrimental to arbitration's fundamental attributes and specificity, if they're not supplemented with the right and reasonable cybersecurity measures. The reality is that the risks posed by the digital world increase with the increase of IT utilization. In turn, the need for more cybersecurity measures and protocols increases as well. All these factors will slowly but surely create more restrictions and barriers on the traditional aspects and attributes of certain mechanisms, but absolutely resisting change and going all out on preserving traditional norms is like swimming against the current, which will be counterproductive.

[71] See https://neuralink.com/

CHAPTER 2: The Omnipresence of Cyberspace and its Influence on Arbitration

Parallel to the concept of data protection with its regulations and impact on ADR proceedings. There exists another deeper, more technical, and multi-layered structure that shields personal data at the infrastructural level in any system in cyberspace. Cyberspace can be defined as the virtual global realm of information. It is made up of an interdependent network of information technology infrastructures, which includes the Internet, telecommunications network, computer systems, and implanted processors and controllers. Understanding the complexity of cyberspace can be simplified by perceiving it as a multi-leveled structure of physical, logical, and social layers made up of five elements distributed among these layers. The physical layer is made up of the geographic and physical network components; the logical layer adds the logical network component, and the social layer adds the persona and cyber-persona components to finish up cyberspaces' dimensions[72]. Accordingly, (Sub-Chapter 1) will be a study of the constituents of cyberspace and its threats that can impact the functional and material aspects of arbitrations. Whereas, (Sub-Chapter 2) takes on the cybersecurity protocol for international arbitration that offers tangible and reasonable remedies for the threats posed in cyberspace.

[72] AcqNotes, Cyberspace, found at https://acqnotes.com/acqnote/careerfields/cyberspace#:~:text=Cyberspace%20is%20the%20global%20domain,and%20embedded%20processors%20and%20controllers. visitation date 17/12/2020

SUB-CHAPTER 1: Arbitration's Procedural and Personal Cyber-Challenges

The purpose of the following section will be to demonstrate how cyber-intrusions have affected the personal and material aspects of the arbitral process. Accordingly, (Section 1) will provide an overview of cybercrimes and the consequences it has on decisions rendered by tribunals following the admittance of unlawfully obtained digital evidence. Whereas, (Section 2) section will analyze whether the presence of cyber-intrusions has altered or modified an arbitrator's duties.

SECTION 1: Understanding Cybercrime and their Technical Consequences

Understanding how criminals operate in cyberspace is a necessary component in figuring out how anyone with access to the digital world can have a huge impact on the actual world and its sectors. For this reason, providing a brief introduction into the essence of cybercrime with some examples (Sub-Section 1) would formulate a coherent chain of thought that leads to the acknowledgment of how cyber-intrusion can yield procedural consequences on extrajudicial methods (Sub-Section 2).

Sub-Section 1: The Essence of Cybercrime

A- Cybercrime (Network Intrusions and Attacks)

To begin with, it's noteworthy to highlight the difference between an intrusion and an attack. An attack can occur without the actual entry to the network or system that is compromised. For example, the denial of service (DoS) or distributed denial of service (DDoS) attacks can paralyze a network without violating its virtual boundaries, through overloading or flooding network resources to make it unavailable for actual users. Understanding the difference between intruding into a system and attacking a system can change the crime description, and could lead to charges being dropped based on wrongful accusations. In the context of a physical crime, it is similar to burglary versus robbery. The crime of robbery needs theft to be accompanied by physical assault,

but burglary is the act of stealing upon unauthorized intrusion into a premise[73]. Second of all, attacks are also of different natures, they fall under several categories like direct and distributed attacks. Direct attacks are instigated from a computer used by the attacker, while distributed attacks are done through someone else's system(s), so it involves intermediary systems which leads to unwilling or unknowing crime participation and victimization[74]. Additionally, attacks can also be manual, automated, or accidental. Unlike manual attacks that require physical steps to be taken by an attacker, automated attacks are performed by a computer program. While accidental attacks could happen unintentionally through experimentation or visiting websites or email links that contain viruses. In some cases, it could be that the virus found in an email sent by somebody is a victim himself in the context of a distributed attack[75]. The most striking aspect of cyberattacks or intrusions is that they aren't always detectable. Some attacks take years to be discovered, while others are never found out. Moreover, it's sometimes extremely difficult to trace the attack or intrusion back to the criminal, especially that cybercriminals operate remotely and can cover their tracks efficiently. Furthermore, cybercrimes have severe consequences on a financial, legal, reputational, and operational level. They could easily cause their targets to face legal conflicts, bankrupt them, cease their operations and damage their reputation beyond customer or consumer forgiveness.

The most common type of attack is malware. Cybercriminals install malicious software to damage and gain access to networks, servers, systems, or any device[76]. Recently, attackers are using social media schemes to launch their attacks and target people who lack awareness, especially now during COVID-19 where everyone is always online. They also use fake COVID-19 advertisements and websites to penetrate and infect a user's system. These attacks could happen in several ways since malware is an inclusive type of attack. For example, it includes the installation of a trojan horse software that deceives users into opening them which would allow

[73] Debra Littlejohn Shinder, Scene of the Cybercrime, Computer Forensics Handbook, Syngress Publishing, Inc., USA, 2002, pages 282-284
[74] Ibid 284,285
[75] Ibid 286,287
[76] Simpli Learn, An Introduction to Cyber Security: A beginner's Guide, E-book, last updated August 24, 2020, page 4, found at https://www.simplilearn.com/introduction-to-cyber-security-beginners-guide-pdf visitation date 17/12/2020

the attacker to gain access to the network or device[77]. Also, viruses and worms are types of malware; their functions mimic those of their biological counterparts after which they are named. Accordingly, viruses multiply and duplicate inside one's network performing harmful acts[78]; whereas, worms replicate and move from one system or device to another[79]. Moreover, cybercriminals use "Spoofing" methods which rely on the alteration and impersonation of other sources or IP Addresses to deceive users into giving up information. In other words, one machine or system impersonates another to allow the hacker to bypass port filters and overcome protective firewalls[80]. Additionally, "Phishing" is also a common type of malware. These attacks rely on authentic-looking messages, bank or company emails, or links that request confidential personal data and when provided install malware programs[81]. Furthermore, an important type of Malware is Ransomware which freezes the entire system and locks out everyone until a ransom is paid[82]. This is similar to taking a computer system hostage. These attacks often happen to governmental sectors since they are the most willing to negotiate on or pay ransoms, due to the critical information they have and the principle of public establishment continuity. Finally, other types include Adware (attacks based on false advertisements) [83], and Spyware (an undetected software that transfers files from one system to another) [84].

B- Noteworthy cyberattacks.

a) Equifax Data Breach (2017)

Hackers gained access to files containing personal and sensitive personal data such as social security numbers, birth dates, drives license, and 2019,000 consumers had their credit card data

[77] Reciprocity, What is Cybersecurity? Online Article, published September 11, 2019, at https://reciprocitylabs.com/resources/what-is-cybersecurity/ visitation date 17/12/2020
[78] Shinder (Debra L.), OP. Cit. supra note 73, pages 337,338
[79] Ibid, page 338
[80] Ibid, pages 297-300
[81] Reciprocity, OP. Cit. supra note 77
[82] Ibid
[83] Ibid
[84] Ibid

exposed. The scope of the breach affected 147.9 million U.S. consumers and reportedly cost the company $4 billion in total[85].

b) Marriott-Starwood Data Breach (occurred 2014- made public 2018)

The attack targeted one of its reservation systems and accessed the Starwood guest reservation database in the U.S. The attackers copied and encrypted information which affected people who stayed in Marriott's 6,700 global Starwood hotel properties since 2014. The attack affected approximately 500 million people[86].

c) Uber Breach (occurred 2016- reported 2017)

Uber discovered that hackers acquired the names, email addresses, and mobile phone numbers of 57 million Uber application users, in addition to the driver license numbers of 600,000 Uber drivers[87].

d) WannaCry Attack (2017):

It is a ransomware crypto-worm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoin cryptocurrency. This was a global attack affecting every organization that hadn't installed Microsoft's security update from April 2017. This attack resulted in an estimated 200,000 infections in over 150 countries. More importantly, organizations such as Boeing Commercial Airlines, Ministry of Internal Affairs in Russia, Spanish Telecom, several governments, and the National Health Service (NHS) in England and Scotland were struck by this attack, affecting their systems and devices such as MRI Scanners, blood storage refrigerators. According to estimates, losses from the attack cost up to $4 billion, while others say that it could be in the hundreds of millions[88].

[85] Equifax Announces Cybersecurity Incident Involving Consumer Information, press release, found at https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628 visitation date 29/12/2020

[86] Michael Simon, Marriott Starwood hotel data breach FAQ: What 500 million hacked guests need to know, Online Article, published in PCWorld, November 30,2018, found at https://www.pcworld.com/article/3324609/marriott-starwood-hotel-data-breach-faq.html visitation date 29/12/2020

[87] Dara Khosrowshahi, 2016 Data Security Incident, November 21, 2017, found at Uber's official website: https://www.uber.com/newsroom/2016-data-incident/ visitation date 29/12/2020

[88] Marlese Lessing, Case Study: WannaCry Ransomware, Online Article, published July 9, 2020, found at https://www.sdxcentral.com/security/definitions/case-study-wannacry-ransomware/ visitation date 29/12/2020

e) Zoom Attack (2020):

This platform became popular in the past year and a half after the COVID-19 pandemic. The pandemic caused the business, teaching, and other sectors which migrated online to use such platforms. However, the Zoom platform was vulnerable to cyberattacks and engaged in deceptive and unfair practices that undermined the security of its users[89]. It was reported that hackers acquired data (credentials, usernames, and passwords) of more than 500,000 users[90].

These attacks and many others have caused massive ramifications on different levels. Entire systems and platforms had to be changed, legal settlements were reached and fines were paid. Entities that were attacked or failed to set up adequate security systems suffered from irrevocable reputational and operational damage. In turn, these attacks, intrusions, and the whole idea of the digital world merging with the real one, introduced a new set of procedural issues that weren't foreseen in the legal sector. This caused different legal sectors to come up with different interpretations which consequently led to different outcomes. The aforementioned premise can be tested out when assessing how the admissibility of unlawfully obtained digital evidence was dealt with in different extrajudicial tribunals in different cases.

Sub-Section 2: Admissibility of Unlawfully Obtained Digital Evidence

The aforementioned overview of cybercrimes and their consequences serve as a foundation to another byproduct of these attacks which influences how justice is carried out. Usually, when cyber-intrusions or attacks are carried out, perpetrators leak classified documents and information that are mostly true and could potentially change the outcome of pending or resolved cases. This phenomenon is overlooked by many, especially in extrajudicial dispute resolution processes. The absence of a clear international arbitration law that yields a unified tribunal approach in matters relating to the admittance, admissibility, and reliability of illegally obtained evidence through IT methods, cyberattacks, or other informal means, requires a study of several case laws to figure out whether different tribunals are implementing a common methodology. The complexity of this issue increases because of the flexibility in which arbitral tribunals

[89] See https://www.ftc.gov/news-events/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement visitation date 29/12/2020

[90] See https://www.forbes.com/sites/daveywinder/2020/04/28/zoom-gets-stuffed-heres-how-hackers-got-hold-of-500000-passwords/?sh=264cc0d55cdc visitation date 29/12/2020

manage their cases. In turn, it results in different appreciation of facts, and dissimilarities in evaluating and weighing the importance of evidence. Additionally, new evidentiary frontiers are being explored, with the traditional rule of law and access to justice in international proceedings. This requires the availability of all relevant evidence to the tribunal. Thus, resulting in different outcomes on similar questions[91].

The use of illegally obtained evidence through the use of modern cyber-intrusion techniques was witnessed in the *Yukos v. Russia*[92] case settled before the Permanent Court of Arbitration (PCA). To issue its award, the Tribunal depended on confidential diplomatic cables from the U.S. State Department published by Wikileaks which supported the claims of Yukos and awarded them damages over $50B[93]. The Tribunal assessed the Wikileaks documents and gave them credibility, however, it didn't address their admissibility which is deemed illegal under U.S. law. In a later case between *Hully Enterprises (Cyprus) v. Russia*[94], the Tribunal implied that unlawfully obtained evidence is admissible before -and may be used by- investment tribunals[95].

Another case that had the same issue *is ConocoPhillips v. Venezuela*[96]. This time after the tribunal had ruled in favor of ConocoPhillips, the Venezuelan government claimed that this ruling should be preliminary and submitted new evidence that exonerates them which was based on Wikileaks derived cables. Accordingly, the Wikileaks cables contradicted the tribunal's

[91] Cherie Blair, Ema Vidak Gojkovic, WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence, Article, published in ICSID Review: Foreign Investment Law Journal, Volume 33, Issue No.1, February 3, 2018, pp. 235-259, found at https://omniastrategy.com/wp-content/uploads/WikiLeaks-and-Beyond.pdf visitation date 4/1/2021

[92] For more on the case, see PCA Case No. AA 227, In the Matter of an Arbitration Before a Tribunal Constituted In Accordance with Article 26 of the Energy Charter Treaty and The 1976 UNCITRAL Arbitration Rules, between Yukos Universal Limited (Isle of Man) and The Russian Federation, Final Award, 18 July 2014, found at https://www.italaw.com/sites/default/files/case-documents/italaw3279.pdf visitation date 4/1/2021

[93] See PCA Case No. AA 226, In the Matter of an Arbitration Before a Tribunal Constituted in Accordance with Article 26 of the Energy Charter Treaty and The 1976 UNCITRAL Arbitration Rules, between Hulley Enterprises Limited (Cyprus) and The Russian Federation, Final Award, 18 July 2014, paragraphs 1189, 1208, 1213, 1218, 1223 found at https://www.italaw.com/sites/default/files/case-documents/italaw3278.pdf visitation date 4/1/2021

[94] Ibid

[95] Blair (Cherie) and Gojkovic (Ema), OP. Cit. supra note 91, page 248

[96] For full case see ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela, ICSID Case No. ARB/07/30, found at https://www.italaw.com/cases/321 visitation date 5/1/2021

findings[97]. This claim was rejected based on the res judicata principle that doesn't allow for the reconsideration of prior decisions under the International Centre for Settlement of Investment Disputes (ICSID) Rules[98]. Once again, silence loomed over the admissibility of evidence obtained through Wikileaks

Commenting on the case, J.H. Boykin and M. Havalic concluded that the previewed silence concerning the suitability of such evidence can be observed as an implicit decision by the majority in regards to their view and methodology in dealing with these types of evidence, especially that everyone is accustomed to seeing every argument raised by the parties re-administered verbatim in the body of the award[99].

Additionally, Professor Georges Abi-Saab expressed his strong opposition to ignoring WikiLeaks cables in this case, and dubbed it as a "travesty of justice that makes a mockery not only of ICSID arbitration but of the very idea of adjudication". He stated that "The revelations of WikiLeaks cables change the situation radically in dimension and seriousness. Here we have a full narrative of the negotiations, with a high degree of credibility" … "It is a narrative that radically confutes the one reconstructed by the Majority, relying almost exclusively on the assertions of the Claimants throughout their pleadings that the Respondent did not budge from his initial offer …" Then he went on to question the tribunal's fairness, and whether it respects the moral task of truth-seeking and justice administration that it was assigned to deliver, after ignoring such evidence and delivering an award based on severely contestable findings. This opinion is an indicator of the inevitable influence that such evidence could have on proceedings and the importance of striking and preserving a balance between the interests of justice, and procedural integrity[100].

---

[97] ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela, ICSID Case No. ARB/07/30, Decision on Respondent's Request for Reconsideration, 10 March 2014. Found at https://www.italaw.com/sites/default/files/case-documents/italaw3119.pdf visitation date 5/1/2021

[98] ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela, ICSID Case No. ARB/07/30, Decision on the Proposal to Disqualify a Majority of the Tribunal 5 May 2014, paragraphs 20, 21. Found at https://www.italaw.com/sites/default/files/case-documents/italaw3162.pdf.pdf

[99] Blair (Cherie) and Gojkovic (Ema), OP. Cit. supra note 91, page 249

[100] ConocoPhillips Petrozuata BV, ConocoPhillips Hamaca BV and ConocoPhillips Gulf of Paria BV v Bolivarian Republic of Venezuela, ICSID Case No ARB/07/30, Decision on Respondent's Request for Reconsideration, Dissenting Opinion of George Abi-Saab,10 March 2014, paragraphs 64, 66,67, found at https://www.italaw.com/sites/default/files/case-documents/italaw3121.pdf

In 2006, a dispute between Libananco (Cyprus Corporation) and Turkey[101] provided a different context to the previous issues. During the proceedings, it was discovered that Turkish authorities were intercepting the electronic communications of Libananco, including those with its legal counsel. Although the Turkish government claimed that these interceptions were part of a money-laundering investigation, the tribunal ordered to dismiss and destroy any intercepted communications concerning the arbitration. This decision was based on upholding principles of fair arbitration which is done in good faith, alongside the protection of confidentiality and legal privileges.

In July 2015 ICISD tribunal in *Caratube International Oil Company and Mr. Devincci Saleh Hourani v. Kazakhstan*[102], awarded Caratube $39.2 million in damages. The Claimants (Caratube) relied on 11 documents- 4 of which were covered by lawyer-client privilege- out of the 60,000 documents leaked after the hack that targeted Kazakhstan's government's computer network. These documents were made public and were considered similar to the document disclosure through WikiLeaks. The issue of admissibility was raised by the Respondent and the documents were labeled as "stolen documents". However, the tribunal decided to allow the admission of all non-privileged leaked documents but excluded those bound by legal privilege[103].

In these two preceding cases, we notice the difference in the Tribunals decision on admissibility was based on the question of who performed the unlawful activities (hacking/ illegal interception) to obtain the documents. In the Libananco case, Turkey committed unlawful activities and relied on their actions to present documents. Whereas in the Caratube case, the claimant relied on publicly disclosed documents through unlawful actions committed by a third party. Additionally, another factor that played an important role in the consideration of illegally obtained evidence was the status of such evidence. In other words, if they were bound by legal privilege, they weren't admissible.

[101] ICISID Case No. ARB/06/8, International Centre for Settlement of Investment Disputes Washington, D.C., In the proceeding between, Libananco Holdings Co. Limited (Claimant) and Republic of Turkey (Respondent), Decision on Preliminary Issues, Dated 23 June 2008, found at https://www.italaw.com/sites/default/files/case-documents/ita0465.pdf visitation date 5/1/2021

[102] See ICSID Case No. ARB/13/13, International Centre for Settlement of Investment Disputes, Caratube International Oil Company LLP and Mr. Devincci Salah Hourani v. Republic of Kazakhstan, September 27, 2017, found at https://www.italaw.com/sites/default/files/case-documents/italaw9324.pdf visitation date 5/1/2021

[103] Ibid, paragraph 158

As seen in this Sub-Section's examples regarding the disclosure and admittance of illegally obtained confidential or privileged information into evidence. Unlawful data access may result in disruptions and procedural obstacles, and undermine the fundamental attributes of the adjudicatory system and its standard due process elements.

In conclusion, while all of the above cases fail to define a clear and explicit standard for deciding on the admissibility of unlawfully obtained evidence, there appear to be some common elements and methodology in dealing with this issue. First of all, obtaining evidence illegally isn't sufficient by itself to disqualify evidence as inadmissible. Second of all, the element that contributed to the Tribunals decision of admissibility of illegally obtained evidence can be summarized by three questions:

1- Did the party involved in the proceedings unlawfully obtain evidence to benefit from them?

2- Is it in the public's best interest to reject the admissibility of such evidence and are they guarded by legal privilege[104]?

3- Do the interests of justice administration favor the admission of evidence[105]?

This segment only offered a preview into a procedural issue caused by the byproducts of the digital age. Admissibility issues of digital evidence only scratch the surface when it comes to the influence of cyberspace on the legal sector. However, it was worth shedding a light on because it is an issue not frequently discussed and has the capability of swinging an important ruling one way or another. In turn, it is an indication that the absence of proper, coherent guidelines with a cooperative mentality will weaken the extrajudicial system when facing off against other more serious challenges of cyberspace. For this reason, the duties and roles of arbitrators have become significantly more important especially since these duties were compiled over time have been in

[104] Based on Article 9(2)(f) of the International Bar Association (IBA) Rules on the Taking of Evidence in International Arbitration (2010), the tribunals are empowered to "exclude from evidence or production and Document" on the "ground of special political or institutional sensitivity (including evidence that has been classified as secrecy by a government or a public international institution) that the Arbitral Tribunal determines to be compelling". Thus, many of the WikiLeaks cables that are considered "Secret" by the US, would therefore meet the requirements of Article 9(2)(f). Hence, it is justifiable for tribunals to dismiss any WikiLeaks-derived evidence on those bases.

[105] Blair (Cherie) and Gojkovic (Ema), OP. Cit. supra note 91, page 259

practice for a significant duration of time. Consequently, it becomes a question of whether arbitrators, as the first line of defense against cyber and normal intrusions, have unambiguous guidelines to confront the threats of cyberspace.

SECTION 2: Consequences of Cyber-Intrusion on Arbitrators

Arbitration is built upon a system of interdependency between a multitude of actors, nations, and legal frameworks. This means that the safety and security of data that falls within the confines of this interdependent system will be measured in relation to the security of its weakest link. Accordingly, with human beings and their devices being the weakest link in the chain of cyber-protection they should be better prepared to handle arising problems. However, arbitration is based on a system of rights and obligations for its participants. Therefore, it is important to begin with the essential duties of arbitrators since they bind the whole process together (Sub-Section 1). Then (Sub-Section 2) will provide evidence that shows how the essence of an arbitrator's duties apply in cyberspace.

Sub-Section 1: The Duty of an Arbitrator to Avoid Intrusion

First off, the process of arbitration isn't uniquely vulnerable to data breaches, but like other sectors and fields that are data-centric, it isn't immune to the persistent threat of cyberattacks. Similarly, focusing on the duties of arbitrators doesn't mean that they bear the sole responsibility of ensuring the safety of the entire interdependent process of arbitration. For, the security of data relies on the responsible behavior and attentiveness of every individual involved. Hence, every actor whether involved directly or indirectly in arbitration can be the weak link, and serve as a gateway for intrusions and attacks. However, as presiding actors, arbitrators have a front-line duty to safeguard the integrity, legitimacy, and security of a process that is appealing to intruders.

A- Arbitrator's duty to avoid cybersecurity breaches- Sources of their Duties

First of all, there are no standalone explicit instructions or obligations that address the arbitrator's or parties' duty of upholding data security against cyber-breaches. However, even though arbitration rules, ethical codes, practice guidelines, and national laws that govern

international arbitration fail to address this issue, they provide a set of well-established arbitral duties that can be implicitly applied in the context of data security. Additionally, cybersecurity obligations may be found in attorney codes of conduct, data protection laws and regulations; party agreements[106]. The three main duties of an arbitrator are:

a) The Duty of Confidentiality

The duty and extent of confidentiality are what set arbitration apart from other methods of litigation. It is based on a legitimate expectation of process confidentiality and privacy of litigation in adjudicatory systems. Accordingly, a breach of privacy committed through cyber-intrusion undermines the legitimate expectation of confidentiality of the arbitral process. Hence, not protecting against cyber-intrusion undermines the confidentiality of the process, which deems this specific duty a natural extension of an arbitrator's confidentiality obligation[107].

b) Duty to Preserve and Protect the Integrity and Legitimacy of the Arbitral Process

An arbitrator's duty to avoid unlawful or unauthorized intrusion falls under his duty to uphold and secure the integrity and legitimacy of the arbitral process. Thus, cyber-intrusion through hacking or any other digital or physical means using IT threatens the integrity and legitimacy of the arbitral process and is therefore subsumed under the arbitrator's original duties[108]. Building on this premise, obtaining and using data through any unauthorized or illegal method, either directly by the parties or indirectly, in arbitration can cause irrevocable damage to the proceedings. Thus, igniting a sense of doubt in the legitimacy of the process.

c) Duty of Competence

There is no denying that an arbitrator has a duty of competence. Several codes of ethics reaffirm this notion by requiring arbitrators to be competent to serve[109]. However, these codes don't define

[106] Stephanie Cohen & Mark Morril, A Call To Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion, Article 11, published in the Fordham International Law Journal, Volume 40, Issue 3, 2017, pp. 982-1012, page 990, found at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2657&context=ilj visitation date 6/1/2021

[107] UNCITRAL Notes on Organizing Arbitral Proceedings, New York, 2016, page 19 7(b), 58, found at http://www.uncitral.org/pdf/english/texts/arbitration/arb-notes/arb-notes-2016-e.pdf visitation date 6/1/2021.

[108] Cohen (Stephanie), Morril (Mark), OP. Cit. supra note 106, page 994

[109] For example, ABA/AAA Code of Ethics for Arbitrators Cannon I; IBA Rules of Ethics for International Arbitrators Rule 2.2; CIARB Ethics Code Rule 4.

competence. Thus, leaving room for broad interpretations. Therefore, expanding the scope of an arbitrator's duty of competency to include digital literacy, and an understanding of the reasonable measures. This duty has become an essential requirement to avoid cyber-intrusions in the highly digitalized and interconnected domain of international arbitration[110].

Additionally, as exhaustively explained in Part 1, data protection laws and regulations that govern how information can be stored, collected, and transferred, have generated additional duties for arbitrators. Although they didn't create explicit or standalone duties, they altered and modified the existing ones to encompass the demands of digitalization. These regulations follow the idea that to maintain user confidence in international arbitration, arbitrators must show their preparedness, competence, and the ability to handle and process sensitive personal data, while also materializing these virtues to the public. Thus, global data protection and security laws and regulations demand proactivity and not reactivity from arbitrators, which is done on a case-by-case basis.

Sub-Section 2: Nature and Scope of an Arbitrator's Duty to Avoid Intrusion

A- A Natural Extension of Essential Duties

The aforementioned insight into the sources of an arbitrator's duties has shown that the duty to avoid intrusion is found in his essential obligations of upkeeping confidentiality, securing and preserving integrity and legitimacy of the process, and competency. Thus, the duty to avoid intrusion in the digital age is a natural extension of what was already required from an arbitrator, but in a broader context. The idea of cybersecurity and digital intrusion is new, but the obligation to avoid these challenges is neither independent nor does it demand an out-of-the-ordinary requirement from arbitrators. In other words, the duty to avoid intrusion doesn't obtrude the particularity of arbitration. The peculiarity of challenges proposed by cybersecurity on the practice of international arbitration is evident through the grouping of different cybersecurity

[110] UNICTRAL Notes on Organizing Arbitral Proceedings, New York, 2016, page 19, paragraphs 56-58 found at http://www.uncitral.org/pdf/english/texts/arbitration/arb-notes/arb-notes-2016-e.pdf visitation date 6/1/2021; ICC Rules, at Appendix IV in reference to case management techniques; ICDR Rules, Article 20.2 (conduct of proceedings with consideration for technology)

responsibilities that are hidden within an arbitrator's original duties. For this reason, proactivity in threat recognition, acceptance of responsibility, and taking reasonable preventive measures is essential in effectively securing an arbitration's cyberspace[111].

B- A Symbiotic Environment Dependent on Independent Duties

As said in the overview of sub-section 1, achieving a complete cybersecurity framework for an arbitral process is an inherently shared responsibility that requires interdependent efforts in securing the weakest link. Compromising any link in the custody of sensitive information has a domino effect that impairs every other participant. For this reason, isolating one participant of the arbitral process as bearing the sole responsibility for cybersecurity, negates the interdependent landscape of digital threats. From the perspective of arbitrators, it is easy for them to consider cybersecurity as an issue for the parties and their counsels that are dealt with on a case-by-case basis since the data entrusted for arbitrators to keep secure are originally from the parties and counsel themselves. Moreover, the fact that the extent of their duties as arbitrators are acquired through party agreements and other rules makes it easier for them to neglect such duties. The parties have a particular role to play in safeguarding their data and assigning specific security precautions for arbitrators to follow. However, an arbitrator has an independent duty in ensuring cybersecurity. As established through their duties, arbitrators under their prescribed obligations and their inherent powers as adjudicators, are the safe-keepers of security in an arbitral process. Additionally, an arbitrator's daily security practices pre-exist individual-case-related matters and continue after the matter is concluded. Thus, regardless of the few overlapping obligations and duties of participants, counsels, arbitral institutions, and third-party service providers, the individual strength of an arbitrator's cybersecurity practices will dictate the overall security of arbitration-related data as soon as he/she becomes part of the case. It is an ongoing duty that precedes setting his case-specific cybersecurity protocols, and continues after the matter is concluded[112].

[111] Cohen (Stephanie) & Morril (Mark), OP. Cit. supra note 106, page 1004,1005
[112] Ibid, page 1005,1006

C- Personal Accountability

An arbitrator's appointment is tailored around his/her characteristics, qualities, qualifications, and reputation[113]. Therefore, there is a link between an arbitrator's qualities and their role as presiding figures over arbitral proceedings, which makes it a personal duty. In other words, it can't be delegated. This is similar to other personal and non-delegable duties of an arbitrator (e.g. duty of deciding a case, attending hearings, deliberations, evaluating party submissions and evidence, or other responsibilities)[114]. Moreover, this notion extends beyond its common use in the inadmissibility of decision-making delegations by arbitrators to their secretaries and can be applied to the arbitrator's cybersecurity duties. Thus, arbitrators must not depend entirely on their institutions or IT service providers for setting and monitoring cybersecurity frameworks, while they absolve themselves from any commitments and responsibilities. Since regardless of the overall strength of the cybersecurity system, its strongest enemy is individual choices and conduct. For this reason, human carelessness and poor decision-making are what intruders feed off of. Hence, every single party involved has a personal responsibility to the entirety of the system and everyone in it. Therefore, dismissing the duties of cybersecurity by arbitrators as a secondary or an IT issue, and totally entrusting them to fulfill the duty to fend off intruders, may reflect badly on their essential duties of keeping the process confidential, and preserving its integrity and legitimacy towards the parties and the public[115].

D- Continuous and Evolving Nature

Usually, duties are confined, they are based on fixed principles that are applicable in a certain timeframe and a specified workspace. However, the duty to avoid intrusion is a continuous obligation that has to be respected at every time and place. The notion of continuity stems from the original duty of confidentiality that an arbitrator must conform to, which extends beyond the lifespan and personal matters of a case. Additionally, reasonable expectations of preventing intrusion and heeding cybersecurity protocols are always in place from a time that predates an

[113] Gary B. Born, International Commercial Arbitration (A Three-Volume Book Set), Second Edition, Volume II: International Arbitration Procedures and Proceedings, published by Wolters Kluwer Law & Business; 2nd edition, The Netherlands, April 22, 2014, page 2013, "Arbitrators are almost always selected because of their personal standing and reputation…"
[114] Ibid, page 1999
[115] Cohen (Stephanie) & Morril (Mark), OP. Cit. supra note 106, page 1006-1008

arbitrator's appointment, since privacy and confidentiality are essential attributes of the arbitral process. Moreover, the evolving nature of the duty to avoid intrusion has its roots in the duty of competency. As seen, because technology is always evolving and new ways to threaten the security and safety of cyberspace are always in development, an arbitrator can't take effective steps to avoid intrusion unless he/she is up to date with the latest developments in the cyberworld. Although this task demands more time, effort, and a willingness to have the capacity to understand a different field of specialization, it is embedded in the origin of their duties and the nature of the process[116].

E- Defined by Reasonableness

According to cybersecurity professionals, today's environment of ever-escalating data breaches changes the context of perceiving cyberthreats. It went from a possibility or a chance of occurring controlled by the practices of individuals to an inevitable act dictated by time. In other words, there is no such thing as a perfect security system, and whether or not a breach occurs is a question of when will it happen, and not whom will it happen to[117]. Practically speaking, arbitrators can't guarantee that arbitration-related information will remain secure, but can only take reasonable steps to limit the continuous risks of cyber-intrusion[118]. For example, the FTC in *LabMD v. Federal Trade Commission*, considered data security as a continuous process bounded by reasonableness and refuted the idea of a singular or perfect data security program, assuring that being breached isn't a violation of the law[119]. Accordingly, this notion is also applicable to an arbitrator's duty of confidentiality, and in the same sense, the duty of arbitrators to avoid intrusion is bound by reasonableness and tailored around the risks presented. Moreover, applying a one-size-fits-all approach and focusing on having a perfect security system may jeopardize the specificity and particularity of the arbitral process on one hand, and render the security system

[116] Ibid, page 1009
[117] International Chamber of Commerce (ICC), Cybersecurity Guide for Business, 2015, page 10, found at https://www.iccwbo.be/wp-content/uploads/2016/05/ICC-Cyber-security-guide-for-business.pdf visitation date 8/1/2021
[118] Ibid, page 4
[119] Federal Trade Commission, FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy, Press releases, August 29, 2013, found at https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers visitation date 8/1/2021

obsolete and counterproductive, on the other hand[120]. Thus, a reasonable approach that is flexible and case-related enables the consideration of different factors and the required trade-offs that are bound to exist between increasing security measures and protecting the essential virtues and principles of the parties and the system as a whole. Hence, finding a balance of conducting the proceedings efficiently, cost-effectively, per party preferences that protect fundamental attributes of the arbitral process and duties of an arbitrator, while administering reasonable cybersecurity measures and protocols will yield desired outcomes.

An arbitrator's duty concerning cybersecurity through avoiding intrusion by taking practical measures to prevent unlawful or unauthorized digital access to arbitration-related information is an obligation of handling the issue with reasonable skill and care rather than achieving a specific purpose or result. A purpose obligation imposes a higher duty since it is an absolute obligation to achieve a specified result, which when breached doesn't require proof of negligence. Accordingly, through the nature and scope of an arbitrator's duty to avoid intrusion, this premise could be verified.

The purpose of the approach taken up until now was to illuminate the complexity of the different layers involved in protecting personal data and safeguarding virtual infrastructures. The layers of protection need efforts from different entities, institutions, national and international actors, and regulations. Once we realized that the first layer of protection was being carefully implanted by the GDPR, and had little influence on the specificity of ADR methods, we delved into a deeper, more intricate set of schemes that causes problems on the infrastructural level, which in turn can lead to the total collapse on any sector. However, it remains to be seen in the next chapter how the specificity of ADR, especially arbitration, holds up against the reasonable remedies proposed to mitigate cyberthreats.

[120] Jim Pastore, Practical Approaches to Cybersecurity in Arbitration, Article 11, published in Fordham International Law Journal, Volume 40, Issue 3, 2017, pp. 1022-1032, page 1024, found at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2658&context=ilj visitation date 8/1/2020

As a final remark, the material, physical, mental strain, and damages that can be manifested in cyberspace through its virtual nature, complex crimes and actors, is in itself a warrant for collective countermeasures to be taken. This Sub-Chapter only focused on two ways that cyberspace has impacted, altered, or caused conflicts in arbitration. However, the damages that could be inflicted by cybercrimes on this institution far exceeds what was presented, especially since the sophistication and frequency of cyberattacks are increasing. For this reason, a collective-based individual, national and international remedial approach must be taken to thwart off cyberthreats. These threats aren't likely going to be eliminated, but their impact and repercussions can be mitigated. Thus, reasonable protocols, threat awareness techniques, and long-term organized strategic individual and global planning must happen to form a secure barrier around personal information and critical infrastructures.

SUB-CHAPTER 2: Arbitral Remedies: Reasonable Cybersecurity Measures

The uniqueness and particularity of ADR methods can be best described as an assortment of traditional concepts with a modernized and adaptable configuration that transcends the confines of normal litigation and meets the requirements of the vast majority of the population. Flexibility, party autonomy, and confidentiality are the foundations of specificity in ADR methods. However, the preservation of these principles in the digital age has proven to be a demanding task that demands global attention. As the digital landscape widens its perimeter, the dependency on its basic functions increases. The increase in IT integration has led to the development of protocols and modern litigation systems to conform with cyberspaces' requirements. For, failing to harmonize with technology would eventually cause the obsolescence of traditional norms. Accordingly, the nature of traditional ADR methods and their fundamental attributes made their transition into the digital landscape easier than other domains or legal practices. In turn, this prompted the international arbitration community to develop protocols and guidelines that help protect the process's integrity, values and people, while satisfying the demands of the modern age. Hence, (Section 1) will give an overview of the data security risks that face arbitration and an introduction to cybersecurity. Whereas, (Section 2) will explore the ICCA-NYC Bar- CPR Protocol on Cybersecurity in International Arbitration.

SECTION 1: Overview of Arbitral Cyber-Risks and the General Coping Mechanisms

This section will give a brief overview of the data security risks that makes international arbitration a target of cybercrime (Sub-Section 1) followed by a synopsis of what cybersecurity is (Sub-Section 2). The ideas covered in this section will serve as basic rundowns or tone-setters on the importance of having the right mindset and toolkit for designing the best possible cybersecurity protocol whether it is used in any domain or arbitration specifically.

Sub-Section 1: Data Security Risks in International Arbitration- Overview

International commercial arbitration usually involves sensitive, commercial, confidential, and personal information of high-profile individuals, companies, and organizations, in addition to information that isn't publicly available that can potentially disrupt markets and impact competition (i.e., trade secrets). Also, information exchanged during arbitral proceedings is culled together in large data sets, which include pleadings, transcripts, evidence, expert reports, witness

statements, memorials, attorney work products, and tribunal deliberations. Moreover, the information presented during arbitral proceedings often belongs to natural or legal persons in different countries, which means that a movement and storage of information frequently occurs between countries through IT tools such as smartphones, tablets, laptops, and cloud services which offer a potential portal for unauthorized outsiders to gain access. Thus, the nature of international commercial arbitration appeals to cybercriminals and increases its susceptibility to cyber-threats.

As a result, cybercriminals may target data curators directly (e.g. arbitral institutions, members of the tribunal, council members, parties, experts, vendors, court reports, etc.,) or attack the digital infrastructure of their organizations. For example, the "watering hole" attack in July 2015 on the Permanent Court of Arbitration's (PCA) website during an ongoing maritime dispute between China and the Philippines, in which hackers implanted a malicious Adobe Flash file on the PCA's website that allowed them to exploit the computer systems that visited the website, causing it to go offline and potentially exposing visitors that entered to data theft[121].

Consequently, data disclosures in this context result in damages on multiple levels. This means that the potential disclosure of trade secrets, commercially sensitive or personal information that may violate laws or contractual obligations between businesses or a business with its customers, cause severe repercussions on companies and individuals nationally and internationally. In particular, unauthorized disclosures can harm the reputational and economic status of the target, impose regulatory sanctions, or negligence claims, and impact the integrity of public securities markets. Additionally, it triggers complex and different data privacy laws, privacy frameworks, and ethical standards, since the arbitral process has international elements. Lastly, data security breaches that result from mediocre or inadequate security protocols, threaten to destabilize the public's confidence in the international commercial arbitration institution as a whole[122].

[121] Luke Eric Peterson, Permanent Court of Arbitration Website Goes Offline, With Cyber-Security Firm Contending That Security Flaw Was Exploited In Concert With China-Philippines Arbitration, Article, published on IAREPORTER, July 23, 2015, found at https://www.iareporter.com/articles/permanent-court-of-arbitration-goes-offline-with-cyber-security-firm-contending-that-security-flaw-was-exploited-in-lead-up-to-china-philippines-arbitration/ visitation date 6/1/2021

[122] Cohen (Stephanie) & Morril (Mark), OP. Cit. supra note 106, page 988,989

Sub-Section 2: Overview of Cybersecurity

Cybersecurity is the practice necessary to safeguard networks, programs, and systems against cybercrime. It is the first line of defense against crimes or attacks committed in cyberspace. Often cybersecurity is confused with data protection because of their relation and end-purpose of ensuring data safety. However, the difference is evident when considering each system's objectives and tasks[123]. The three pillars of cybersecurity are to safeguard the availability, confidentiality, and integrity of digital assets and software against internal or external threats in an organization[124]. Whereas, data protection is a set of directives, laws, regulations, and guidelines that manage and dictate how processing of personal data is lawfully conducted to avoid misuse, distortion, or any action that risks the spread of personal information contrary to consent protocols. Building on that, cybersecurity is a broader mechanism that starts at the infrastructural level, since it protects the system that holds the data. Whereas, data protection laws protect against the misuse of data itself. Thus, bypassing cybersecurity safeguards puts personal data at risk. Additionally, cybersecurity breaches could be internal or external, but data protection violations are done accidentally or purposefully through negligence or misuse of personal data. For example, in *FTC v. Facebook*, data was being misused and inadequate measures were taken by Facebook to safeguard data subjects' data which violated data protection laws and resulted in a $5B fine[125]. Whereas, in the Equifax case, proper security measures weren't taken, which resulted in a breach of their systems that lead to data loss[126].

The five most important categories of security that are essential to any state, organization, business, and even individuals are: application security, network security, operational security, information security (physical and digital), and end-user education. Each one of these deals with a certain aspect of security as shown in their names. For example, Information Security (InfoSec) aims to protect sensitive business information from any alteration, loss, or disruption. InfoSec is

[123] Analytics Insight, Data Protection vs. Cybersecurity: Why You Need Both, Online Article, published August 29, 2020, found at https://www.analyticsinsight.net/data-protection-vs-cyber-security-why-you-need-both/ visitation date 17/12/2020

[124] Simpli Learn, OP. Cit. supra note 76, page 2

[125] Federal Trade Commission, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Press Releases, July 24, 2019, found at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions visitation date 18/10/2020.

[126] Federal Trade Commission, FTC Sues Cambridge Analytic, Settles with Former CEO and App Developer, Press Releases, July 24, 2019, found at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer visitation date 18/10/2020.

achieved through several processes and tools implemented to preserve the integrity and privacy of data during transfers and in storage. It encompasses several security procedures such as cloud security, application security, cryptography, infrastructure security, incident response, and vulnerability management[127]. Accordingly, as part of an integrated system of InfoSec and operational security, it is recommended that each company or organization adopt a system of best practices such as organizing sensitive data, awareness of possible threats to their systems, analyzing security cracks and vulnerabilities, assessing the threat level of each potential liability, creating and implementing proper countermeasures to prevent or mitigate any risks. Entities should adhere to and apply operational security methods such as but not limited to: limiting or restricting access to data, compartmentalizing data related jobs so that individuals who are tasked with data security aren't the same ones who work on the organization's network (dual control systems), adopting automated task performing systems to reduce human intervention and minimizing negligence or human mistakes, and implementing incident response and disaster recovery protocols[128]. However, the most concerning aspect of security in relation to the topic of this dissertation is end-user education.

Human errors are huge contributors to data breaches. They manifest several ways like easily falling for phishing schemes, letting unauthorized users access corporate devices, poor password practices, poorly managing high privileged accounts, or leaving devices unsecured and unattended, etc. So, regardless of the strength of security protocols, practices, and systems set up by companies, people will still make mistakes that could prove costly. Thus, individual users should partake in cybersecurity by taking reasonable measures to prevent them from being easy targets. Users should keep their software and operating systems updated, install antivirus software, use strong passwords, never open attachments in spam emails or skeptical links and websites, check security standards before giving out sensitive and personal information, contact companies regarding suspicious or out of place requests, and limit or stop the use of public internet and unsecure

[127] Cisco, What is Information Security? Online Blog, no publication date, found at https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html visitation date 17/12//2020

[128] Ellen Zhang, What is Operational Security? The Five-Step Process, Best Practices, and More, Data Guardian's Digital Guardian Blog, published December 1, 2020, found at https://digitalguardian.com/blog/what-operational-security-five-step-process-best-practices-and-more visitation date 17/12/2020

networks. In general, users should keep their guard up when dealing with network or internet-related devices which account for everything these day[129].

Companies and organizations spend huge amounts of money to try to put in place the most secure and sophisticated systems of protection against cyberattacks, but the fact remains that all those systems could be bypassed by simple human carelessness or errors. Cybercriminals are aware of this fact and target individuals that work or are in a relationship with the threatened company. For this reason, attacks that happen through targeting individuals through "phishing" are so common and dangerous. Thus, educating employees on cybersecurity through special programs and mandatory training courses is crucial. Hence, the strength of a company's security is measured by the strength of its weakest link[130].

SECTION 2: The Framework of the ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration

The cybersecurity protocol is of a very technical nature. It forces the arbitral tribunal, the parties, and everyone involved in the process to take precautionary steps and measures to preserve and secure the system in its entirety and their personal information. Accordingly, the guidelines of this protocol aren't out of the ordinary practices that would require specialized knowledge in the IT field. They are a different manifestation of physical protective practices that are expressed in a digital format. Thus, the requirements for a secure cyber-environment found in the ICCA-NYC Bar-CPR Cybersecurity Protocol offer basic, modernized, and reasonable remedies for mitigating cyberthreats, while preserving the specificity of the arbitral process. Studying the protocol will be divided into two subsections, the first being a discussion of its framework, and the second, a display of the best-recommended practices.

[129] Matt Middleton- Leal, Top 5 Human Errors that Impact Data Security, Article, published in Cyber Chief Magazine, Edition 5, March 2019, pages 5-8, found at https://www.netwrix.com/cyberchief_magazine.html visitation date 17/12/2020

[130] Lawrence King, Why Cybersecurity Education for Employees is so important, Online Article, published July 30, 2019, found at https://www.cyberdefensemagazine.com/end-user-security-education/ visitation date 17/12/2020

Sub-Section 1: The Principles of the Cybersecurity Protocol

-Overview of ICCA-NYC Bar- CPR Cybersecurity Protocol

The main intention behind drafting this protocol was to provide a framework to determine the reasonable information security measures implementable on individual arbitration matters. Additionally, the protocol is intended to increase awareness of information security (InfoSec) in international arbitration. For this reason, the protocol addresses awareness in different contexts throughout its 14 principles and 6 Schedules such as alertness to different physical and cybersecurity risks posed by the nature of arbitration and the type of parties involved, awareness concerning the importance of information security in preserving the public confidence in the process, as well as its integrity; attentiveness to the readily available information security mechanisms to improve daily security practices, awareness of the crucial role performed by individuals involved in the arbitration in efficiently mitigating such risks. Moreover, while this protocol was drafted with international arbitration as its reference, it may be applied to domestic arbitration matters and/or investor-state arbitrations[131].

A- Scope and Applicability of the Protocol (Principles 1-4)

The main virtue of the protocol is that it promotes the notion that information security (physical and digital) is a collective duty and it should be done with reasonableness. Accordingly, it aims to preserve and make use of the fundamental attributes of ADR and ODR such as party autonomy, flexibility, and confidentiality. The application of reasonable information security measures safeguards these attributes, promotes the credibility of the process, and protects the integrity of extra-judicial functions. Concerning its status, the protocol doesn't supersede the applicable law, arbitration rule, institutional regulations, professional or ethical obligations, or other obligations of a binding nature. The nature of arbitration, especially international arbitration, forces the exchange of information between different people and entities that aren't subject to the same legal requirements. Thus, due consideration must be given to the different legal regimes that apply to natural and legal persons, whether directly or indirectly, locally or internationally. As seen in the

[131] The ICCA Report No. 6: ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration, 2020 Edition, found at https://cdn.arbitration-icca.org/s3fs-public/document/media_document/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_electronic_version.pdf visitation date

previous part, there is a myriad of data protection laws, with the GDPR being the most prominent example of rigorous implementation locally and specific adequacy requirements for international data transfers. Accordingly, non-compliance with these laws or any other regulation or binding rule, in favor of applying the protocol or any non-binding guidance may result in substantial penalties, litigation risks, or administrative violations according to the nature of the breach. However, while different data protection laws and other obligations that supersede this protocol differ in context and their specific requirements, almost all of them require the implementation of reasonable data security measures to safeguard the processing of personal data. Hence, it is recommended to consider how concepts of reasonableness, adequacy, proportionality, and appropriateness are addressed in these laws. For those reasons, the principles in this protocol aren't based on a one-size-fits-all arrangement. They provide a guiding framework of reasonable information security measures.

B- Determination of Reasonable Information Security Measures (Principles 5-8)

The individualized approach followed throughout the protocol in determining the necessary implementation mechanisms for information security demands balancing opposing considerations such as cost and convenience. These choices are made on a case-by-case basis according to parties' agreements and case requirements. Accordingly, when determining reasonable information security measures, the parties and the tribunal should give due consideration to:

a) The risk profile of the arbitration

The risk profile of the arbitration is exemplified through the nature, type, importance of data (e.g., normal personal information, sensitive information, confidential commercial information, or information bound by confidentiality privileges or agreements) that is going to be processed during the proceedings, and the legal regime the govern the special types of information. Additionally, the risk that accompanies the subject matter of the arbitration or the identity of the parties, key witnesses, or other participants. For example, the subject matter of the arbitration could concern high-value confidential information (e.g. trade secrets, health care matters, financial records of banks, or law firms), or the persons involved could have a high profile (e.g., celebrities, high ranking officials, public figures) or they could have a history of being targets of cyberattacks. Other elements that could factor into the equation are the nature, size and value of the subject

matter, the security environment of the related persons or entities, and the frequency of information exchanged between countries. These factors in addition to many more case-dependent features must be taken into consideration and be made aware of by all involved parties as part of the risk profile of the arbitration to set up an all-inclusive cybersecurity protocol.

b) The existing information security practices, infrastructure, and capabilities of the parties, arbitrators and any administering institution, and how they address major issues

Several issues need to be addressed and well managed such as, encryptions, asset management, access controls, communication security, physical and environmental security, operational security, information security, and incident management. Accordingly, evaluating the day-to-day security practices and digital infrastructure of everyone involved in the arbitral process is recommended since having an adequate level of security that complements different scenarios and cases could exempt them from applying additional measures.

c) The burden, costs, relative resources of the parties, arbitrators, and any administering institution, as well as the proportionality relative to the size, value, and risk profile of the dispute

It is uncommon for parties, arbitrators, and institutions to have similar technical and financial resources or capacities. Thus, it is important to balance such limitations and reach compromises with all other relevant aspects of the case.

d) The efficiency of the arbitral process

This is the most important consideration that upholds the principle of reasonableness. In cases where the proposed information security measures are cumbersome to the extent that they may obstruct the normal flow of the arbitral proceedings call for grounds to stop or limit their adoption by parties or institutions.

Additionally, in some cases, reasonable security measures can be influenced by the risks present in different aspects of the arbitrations such as, but not limited to, information exchanges and means of transmission of arbitration-related information; storage of arbitration-related information; travel

issues; means of conducting hearings and conferences; and post-arbitration document retention and destruction.

C- The Recommended Procedural Steps to Address Information Security Issues in an Individual Arbitration. (Principles 9-13)

In these principles, the protocol reaffirms essential arbitration attributes and basic tribunal duties while demonstrating how information security measures are agreed upon and integrated in the arbitral process.

a) Party Autonomy

Principle 9 highlights the importance of party autonomy by recognizing that the parties should attempt in the first instance to agree on reasonable information security measures. Thus, as in any other arbitral matter, parties and their representatives will take the lead in deciding on the necessary information security measures applicable to their case, since they are in a position to know what measures suit their case and can be reasonably implemented in a way that preserves the process and ensures their compliance. Parties' legal representatives should deliberate on the implementation of information security issues. These issues will naturally converge with other natural procedural matters, requiring discussions with their clients to reach a balanced and proportional outcome.

b) Preferred time to raise information security issues

Information security should be raised as early as practicable in arbitration. This means that information security issues should be discussed with the parties and the institution, in preparation for, and during, the initial case management conference or procedural hearing. However, in instances where the initial procedural hearing or case management conference is considered too late to raise information security issues, such matters may be raised by the parties for tribunal consideration at any time. Nevertheless, during the initial conference, the arbitral tribunal should be ready to discuss information security matters with the legal representatives of the parties regarding their reasonableness in regards to the case, the preparedness of its members to adopt specific security measures, the disputes arising from adopting certain measures, the tribunals own interests, as guardians of the arbitral process, in preserving integrity and legitimacy of the process, by weighing the parties' concerns and preferences with principles of fairness and equality when

committing to specific information security measures; and address any information security issue it deems influential on the arbitral process. Additionally, arbitral institutions can raise issues of information security with the parties or the tribunal at any time, when they administer over a case.

c) The Tribunal's Authority

The arbitral tribunal has the authority to determine the information security measures applicable to the arbitration. Normally, it is expected that the tribunal will give out directions concerning information security in an early procedural order. However, it may as well, approve and order an information security agreement to be drawn up by the parties. Additionally, the tribunal is tasked with resolving any disputes concerning information security measures or their adoption either arising from party agreements or decided upon by the tribunal itself. Moreover, if a dispute occurs after the arbitration is concluded, it is recommended to set a dispute resolution mechanism that will apply in the event the arbitral tribunal has an expired mandate prematurely during the dispute concerning information security measures. Furthermore, bearing in mind the hierarchy of laws that supersede this protocol, the agreement reached by the parties regarding the adoption and implementation of certain information security measures should be respected by the tribunal if there aren't significant countervailing considerations. However, the parties can't individually bind either the arbitral tribunal or the institution administering the process. Thus, information security agreements concluded by the parties should be deliberated on with the tribunal and, if necessary, any administering institution before its formalization. For example, the tribunal could reject the parties' agreement in circumstances that pertain to the limited capabilities of the arbitrators and the governing institution; for purposes of protecting third-party interests, or for the protection of the legitimacy and integrity of the arbitral process as perceived by the tribunal. Last but not least, it's within the tribunal's authority to modify previously established information security measures, at the request of any party or based on its initiatives, after consultation with the parties and any administering institution, due to changing circumstances. It is well known that the digital landscape is constantly changing and evolving and that the arbitral process could take years to be concluded. Thus, the agreed upon information security measures aren't fixed, as they are open to change under circumstances that may cause a change in the applicable law, the nature of the processed data, the institutional rules, technological developments, case-related risks, etc. Finally, the arbitral tribunal may, at its own discretion, impose sanctions; allocate related costs among parties in the event of a

breach of the information security measures or due to the occurrence of an information security incident. However, such authority is subject to and may be limited by, the applicable law and other superseding regulations.

D- Liability Issues. (Principle 14)

As established, the protocol isn't intended to establish any liability or liability standard for any purpose including, but not limited to, legal or regulatory purposes, liability in contract, professional malpractice, or negligence. It is a non-binding guideline subject to any overriding obligations that may exist. However, this doesn't mean that there are any limitations to the right of the parties to make agreements that allocate liability for security incidents (under the principle of party autonomy), nor does it limit the tribunal's authority in issuing directions regarding matters like costs or sanctions, as previously discussed.

Sub-Section 2: Essential Baseline of Security Measures and Practical Implementations (Schedules A/B/C/D)

The Cybersecurity Protocol offers all custodians of arbitration-related information a non-exhaustive checklist of baseline measures that should be adopted in their day-to-day use of technology in arbitration-related activities. While these measures are important to implement, they should be weighed against the size of the threat, the risk profile of the case, the ever-evolving reality of technology. Additionally, such measures should not obstruct systems, processes, policies, and procedures already in place. Moreover, implementing information security measures is a collective duty, so consultation concerning security matters is advised. Furthermore, these measures are easily and readily accessible and do not require a level of specialization and technicality to understand and implement them. Finally, arbitration-data custodians aren't required to administer every measure on the checklist to every case.

A- Knowledge and Education

a) Staying acquainted with security threats and solutions

The constant development of technology with its peaks and perils makes sustaining suitable security an ongoing process. Thus, keeping abreast with security threats and solutions is

recommended. It could be done through basic subscriptions to newsletters and email alerts from cybersecurity and data privacy practice groups and law firms, or routinely engaging in cybersecurity training according to one's domain of practice, which has become commonly adopted in workplaces (employee training) or through independent organizations.

b) Consider professional duties relating to cybersecurity

As mentioned in the previous sub-chapter, an arbitrator's duty of avoiding cyber-intrusion is a natural extension of his/her duties of confidentiality, competence, and preserving the integrity and legitimacy of the process.

c) Consider industry standards and governmental regulations

Due considerations must be given to governmental standards and country regulation, which will provide help, insight, tools, and readily available procedures to implement. Moreover, these measures and regulations may require the adoption of specific technical standards in certain types of cases that may be addressed during the arbitral proceedings.

B- Asset Management

a) Awareness of assets and architecture:

One should know his own data infrastructure, including professional and personal networks, systems, and devices (e.g., routers, firewalls, software versions, type of laptops and computers used, USB drives, internet provider service, cloud services, remote access tools, back-up services, etc.). Additionally, arbitrators should know where data is placed and have a well-organized inventory. For example, if an arbitral uses a personal tablet to review case-related information, he/she should know whether the documents are stored locally on the tablet, on a server for applications that are used to review these documents, and/or on a cloud storage service. Moreover, it is not enough for couriers of arbitration-related information to be dependent on their organization's responsibility to handle security issues and provide standards and solutions to privacy concerns in the workplace, for security isn't bound by time, place, or people. These individuals will need to consider data flow and security in connection with their personal devices and infrastructure that is used at home for any purpose.

b) Identification of sensitive data and taking steps to minimize and protect it

At this point, identifying sensitive data and effectively managing it is a given. As in data protection regulations, data minimization would decrease the risk of unauthorized access and control. It could be done in several ways such as redaction (masking) of any information deemed personal or sensitive and relevant to the case, or adding confidentiality designations to the names of documents or folders.

c) Avoiding unnecessary multiple copies of documents

In addition to the copies intentionally made by users, several copies could be made and stored without the user's knowledge, especially when devices are linked to software services such as iCloud, Adobe Creative Cloud, Microsoft Cloud, etc.

d) Committing to document retention and destruction practices

Data no longer needed should be securely destroyed. This applies to physical shredding of documents and emptying digital "trash" folders. Securely deleting means that sometimes after deleting information once they can still be recoverable, so using special programs to over-write deleted data to dispose of particularly sensitive data is recommended.

e) Enable remote location tracking and data wiping functions

Applications and tools such as: "Find My iPhone" or "Find My Mac" on Apple devices, and "Find My Device" on Android and Windows are useful in locating misplaced or stolen hardware.

f) Minimize access to sensitive data during traveling

Measures that could help in limiting access to sensitive data during travel include, turning laptops and devices off before passing through border security, forbidding automatic loading when a device is turned on, using full disk encryption; traveling with "burner" or "clean" devices that don't have anything on them and later remotely access information through cloud or email services, also taking only what is needed; marking and segregating confidential information in separate digital folders and asserting applicable privilege or confidentiality protections if asked about them.

g) Backing-up data

A recommended approach is the 3-2-1 rule, which means there should be three copies of the data in total, two different storage media should be used (physical external and encrypted back-up drive), and one copy should be stored offsite (e.g., in the cloud). Additionally, a back-up should be kept offline in case one's network is compromised.

C- Access Controls

Access Controls are used to determine who has authority to access accounts, devices, and information and what privileges they have regarding those accounts, devices, and information. For example, applying strong and complex passwords (at least 8 characters with numbers, letters and symbols) while changing them regularly, using multi-factor authentication, secure password storage mechanisms, and user account management tools (that create separate administrator and user accounts). The development of biometric identification on devices has increased security standards (e.g., fingerprints, face recognition, retinal scans).

D- Encryption

This process uses an algorithm that renders information unreadable to unauthorized persons. To decrypt the information, it needs one or more encryption "keys". Thus, encrypting arbitral information is important especially during transit. For a better level of protection, one should administer file-level encryption, full-disk encryption, and encrypting data in the cloud.

E- Communications Security

a) Users should consider secure file-sharing services instead of emails

Services such as third-party cloud storage applications allow for remote access of data. The use of reputable cloud services with appropriate security controls can be a convenient and better way of data access and sharing than regular emails.

b) Avoiding public networks or, if necessary, limit risks of use:

Public internet networks in hotels, airports, coffee shops, and elsewhere are often unprotected. Consequently, hackers will often target these places to gain easy access to their targets' devices through unprotected Wi-Fi networks. Thus, it is recommended to use mobile hotspots; reliable and paid for virtual private networks (VPN) to establish an encrypted connection over the internet; access websites that use HTTPS security (hypertext transfer protocol secure and encrypts the transmission of data between two devices over the internet); check the authenticity of the network with the owner, and if bound by necessity, limit the length of connection time.

F- Physical and Environmental Security

Physical access to information resources should be properly managed and secured to avoid unauthorized admission, harm, or interference. For this reason, users should lock devices, secure paper files, refrain from leaving documents unattended, use privacy screens for laptops and mobile devices when accessing confidential information or accounts when in public, be aware of the risks that accompany the use of portable storage media that could be easily misplaced or stolen, and never use storage media that is from an unknown source or found randomly in places.

G- Operations Security

Arbitrators, parties, and administering institutions should regularly monitor their security standards and run tests to check for vulnerabilities. Additionally, they should take basic practical precautions to avoid unnecessary risks such as: using professional, commercial products and tools rather than the free ones, forbidding the sharing devices and accounts, immediately installing software updates and patches that are usually patched with the latest security mechanisms that could greatly limit the exposure to cyberattacks (as seen in the WannaCry attacks where it affected users of an older software of Microsoft Windows), and guard digital perimeters using firewalls, antivirus, anti-malware, and anti-spyware software.

H- Information Security Incident Response

The inevitability of being targeted by cyberattacks obliges the consideration of having an incident response plan prepared in advance that includes specific protocols and procedures for

dealing with a breach. Usually, applicable laws and professional or ethical obligations may impose breach response stipulations. Finally, it is better to consider procuring cybersecurity risk insurance, which may be available through bar associations or other sources.

I- Utilization of the Cybersecurity Protocol in the Arbitral Agreements (Schedule D)

a) Arbitral Agreement language.

It is not recommended to decide upon a definitive format concerning information security in the arbitration agreement because of the evolving nature of technology that always produces new mechanisms and poses new risks. Additionally, since the adoption of specific information security measures is based on certain circumstances and an analysis of the case's risk profile. Thus, in this early stage, it is preferable to generally adopt the notion of applying reasonable security measures in the conduct of the arbitration.

b) Agenda of the Initial Case Management Conference or Preliminary Hearing

If information security hasn't been addressed before the preliminary hearing or case management conference, it should be placed on the agenda. Accordingly, the tribunal should issue directions as to the consideration of certain information security protocols (i.e., this cybersecurity protocol) and whether it orders any particular information security measure to be taken in this case. In turn, the parties must deliberate on the subject and submit to the tribunal any agreement or disagreement in regards to what information security measures are reasonable for the arbitration.

c) Agreeing on the specific information security measures.

After considering any agreement reached by the parties concerning the use of reasonable information security measures, and after considering each parties' position concerning the need for additional security measures, the tribunal may choose to address information security in several ways, including these 3 different cases:

1- Parties agree on the reasonable information security measures for the arbitration: In this case, the Tribunal reaffirms the clauses of the agreement on the adoption of information security, and details the additional measures agreed on that were either administered by the parties themselves, or those that were directed by the tribunal, or both.

2- The tribunal prescribes reasonable information security measures for the arbitration: In this case, the parties don't agree on reasonable measures of information security, after being invited by the tribunal to consider information security for arbitration, including whether the tribunal should order any specific security measure. Thus, the tribunal, after considering each parties' respective position, shall direct them to implement the security measures as seen fit, reasonable, and adequate in relation to the risk profile of the arbitration, by the tribunal.

3- Parties agree that existing information security measures are reasonable for the arbitration: In this case, the Tribunal takes note of this course of action taken by the parties. It can state that parties deemed information security measures that are normal in a business context can be reasonably applied in their arbitration, and no additional information security measures are necessary.

d) Post-Arbitration Dispute Resolution Clause

The parties should be aware of disputes that may arise concerning certain information security measures that were agreed upon, after the mandate of the tribunal has ended (i.e., *functus officio*). For this reason, the parties should address the resolution of disputes of such nature early on. They could agree that any dispute that arises after a final award has been rendered or otherwise the tribunal's *functus officio* relating to information security, including, but not limited to, disputes as a result of data breaches or incident response due to or relating to the concluded agreement, including the interpretation, breach, termination, or validity of such, shall be resolved by arbitration.

With all that being said, cybersecurity isn't a one-stop destination. It is an ongoing journey built on preventive methods, constant awareness, collective efforts, and shared responsibilities. The influence of cyberspace and IT integration witnessed in this chapter has both positive and negative aspects; we can't choose to take one without the other. Additionally, we can't escape the integration between the traditional and the modern in this age. In other words, hanging onto outdated means of dispute resolution or any other analog system in fear of change and being exposed to the negative side of cyberspace will be futile. For this reason, projects such as the Cybersecurity Protocol and other initiatives should be welcomed. This protocol is trying to prepare

the ADR industry into migrating smoothly into cyberspace by mitigating risks as much as possible on an individual level. It is also promoting a reasonable approach made available by the adaptability of ADR methods and would benefit its traditional foundations. Moreover, it's reiterating the notion of unity, joint solutions, and cooperation that is essential in any ADR process and has proven to be a key factor in protecting from cybercrimes. Thus, the specificity of ADR, which was feared of being ruined in the modern age, has made ADR in a way more resilient in face of a total overhaul and loss of traditional identity. However, adaptability is a dangerous path to trek on. Adaptability allows for freedom on the spectrum of digitalization, but absolute freedom could cause chaos. Accordingly, it all depends on the extent to which data protection laws, IT integration, and cybersecurity rules are allowed to be engrained in ADR, since if left unregulated or ungoverned it could have the potential to negatively influence these systems.

Conclusion

The purpose of this dissertation was to establish whether and to what extent have data protection laws and privacy regulations, cybersecurity protocols, and the overall shift towards a digitalized world impacted the specificity and particularity of ADR. It would seem that there isn't an explicit answer that directly supports or renounces this question. However, throughout the thesis, it was evident that the fundamental characteristics of ADR weren't on a collision course with these new revelations. In my view, the specificity and uniqueness of ADR's characteristics were essential in preserving the very same characteristics that were expected to be altered. In other words, the individual pillars that shape up ADR's particularity such as flexibility, party autonomy, and confidentiality provided a shield that conserved the totality of these processes, and at the same time allowed for a smooth amalgamation with data security laws and cyberspace. For instance, when the GDPR was applied on national and international arbitration in Part 1 (Chapter 2) it was apparent that, regardless of the lack of explicit mentioning of arbitration in the GDPR, traits such as flexibility and part autonomy were essential for allowing the process of arbitration to fully apply and satisfy the GDPR's broad jurisdictional scope of application and its rigid cross-border data transfer policies. Also, the data controller's obligation and other conditions under the GDPR didn't add extraordinary tasks on arbitrators that would confine the flexibility and autonomism of their duties and the process as a whole. The accumulation of the pre-existing agreements, paperwork, and obligations, with new agreements and stipulations of the GDPR, might add time, cost, and result in additional points being a subject of opposition and dispute, which renders flexibility and part autonomy a double-edged sword. However, the inseparability between the right to privacy and the right of data protection, coupled with the accessibility and ease in which information in today's world can be acquired and misused, have caused such obligations to be essential in concluding any contract. Therefore, the added agreements and obligations that might complexify ADR processes are necessary for the protection and mutual benefit of the involved parties. Hence, the flexibility and part autonomy that shapes up the arbitral process has helped in the realization of the GDPR's full potential that wasn't limited by them. From one perspective the GDPR decreased the absolute freedom and flexibility that parties and arbitrators enjoyed, but from another perspective, it increased the flexibility of the process by offering more options and details to agree upon that weren't in consideration.

Similarly, the same verdict can be reached in the application of the cybersecurity protocol and other cybersecurity measures on ADR. The traits that make these processes unique also proved to be essential in preserving the security of the process at an infrastructural level, the lack of which would've been costly on everyone who is directly and indirectly involved. It was discussed that the duty of arbitrators to avoid cyber-intrusions was embedded in their original duties as arbitrators. This means that the specificity of the arbitral process perceived from the flexibility it offered arbitrators to conduct their practices, allowed for arbitrators' duties to expand beyond their intended purpose. Thus, these duties weren't confined, dramatically altered, or complexified. Under the particularity of the arbitral process, they were flexible enough to be interpreted to conform with cybercrimes. However, confidentiality, flexibility, party autonomy, the lack of establishing precedents, and the absence of clear arbitral rules, had a negative impact when it came to agreeing on the admissibility of evidence obtained through cybercrimes. On the remedial front of cyberspace "reasonableness in application" was the overwhelming message being promoted by the cybersecurity protocol. The promotion of reasonableness in applying cybersecurity measures was essential in preserving the essence of arbitration. Since in mitigating cyberattacks, the traits that make arbitration unique, are the very same traits that would cause its downfall. The nature of cyberattacks makes them unstoppable, especially since they feed off of human mistakes. Essentially, this makes cybercrime a direct consequence of human behavior or lack of which. Accordingly, the extent of flexibility and party autonomy offered in arbitration is directly linked with being more exposed to cybercrimes. Thus, cybercrime in ADR increases or decreases according to the increase or decrease of the flexibility demonstrated in its processes. In turn, this directly affects the specificity of the process. The predicament that faces ADR is that they can't guarantee the prevention of cybercrimes, and the best chance in limiting them is having extreme restrictions on party autonomy and flexibility which would be counterproductive to the process. Hence, following a set of reasonable remedies to mitigate the threats and consequences of cybercrime is the best option to preserve the essence of these processes.

Finally, concerning the influence of IT integration with ADR, the specificity and particularity of ADR proved pivotal in the transition to online-ADR and total ODR. The change caused by the global shift from analog to digital has had a profound impact on all the elements that make up and solve a dispute. The borderless nature of disputes, the increase in low value and medium value disputes, the subject matter of disputes, and the diverse entities and jurisdictions involved, weren't

solvable using traditional means. However, the specificity of ADR methods allowed them to overcome those barriers and migrate into the virtual world to resolve its disputes. The conformity of ADR with digitalization and its modification to ODR in cyberspace is attributed to the core principles it was built upon. This relatively smooth transition from ADR to ODR isn't perceived in the judicial systems, which can be attributed to the judicial system's lack of dynamism displayed in ADR. Hence, technology with its new challenges, consequences, disputes, and remedies didn't change the essence of ADR. The specificity of ADR propelled it to conform with the digital age, as they were either utilized outside the norm of traditional means or were modified in a harmonious, reasonable, and preserved way.

Recommendations

1- Concerning the GDPR and ADR

- The GDRP is a unilateral regulation with a borderless jurisdiction that uses broad terminologies. Although it needs to be that way in order to fight against the borderless nature of the digital world and the constant movement of data and new technologies. However, rather than unilaterally regulating this field and forcing its implementation on a connected world identified by globalization. There should have been a more collective approach to data protection, that takes into consideration the difference in national capabilities, priorities, legal hierarchies, and beliefs, especially since data protection and privacy is a subject of debate in regards to its societal and legal status. Thus, it is recommended to amend the regulation in a way that promotes harmony not just between states within the EU, but with international actors. The amendment should be based on compromises and not single-minded opinions.

- Since the EU has embarked on a journey of regulating a borderless issue, they should start an initiative that aims to assess the impact of EU legislation on third countries, especially developing countries, in data protection and other related fields. The purpose of such an initiative is to gather input and information on EU legal developments that will help them improve the utilization of regulations with international influence.

- The EU should put in place a strategic plan and help other countries follow it for them to achieve good adequacy standards for international data transfers. It shouldn't be approached as a matter of whether a country is adequate or not, and if it's not data can't be transferred. Just like the cybersecurity strategies that the EU and U.S. have in place that aims to help third counties have a better cybersecurity infrastructure. This approach in data protection will promote harmony and increase the flow of data between countries which will be beneficial for both sides. Hence, offering a safer environment for data and data subjects.

- It is also recommended to develop an online database of court decisions and opinions from all around the EU that interprets the principles of the GDPR and how are they employed. The interpretations found in the GDPR, especially in the Recitals are broad and vague. Thus, the need for a more practical guide would allow for a better understanding of the regulation, which would lead to better adherence, and consistency in application.

- Arbitration and other ADR methods should be explicitly recognized in the GDPR. It is believed that Arbitration isn't the popular method of dispute resolution in the EU. However, the EU can't omit or implicitly refer to ADR processes in the GDPR, especially since the GDPR has an extraterritorial reach. First of all, the recognition of arbitration and other forms of extra-judicial dispute resolutions will limit the interpretations and the process of figuring out if that arbitrator is impacted by the GDPR or if he can handle GDPR cases, and the same applies to everyone involved. Second of all, as seen, the flexibility of arbitration allows for its direct application on GDPR cases, which at least warrants its explicit recognition. Additionally, ADR methods can serve as a preventive mechanism that stops data misuse before it happens or before it does any harm to data subjects, especially since time is of the essence in these types of cases. So, figuring out and handling a dispute involving data misuse before, and mitigating those differences before enforcing a hefty fine on the violator will be beneficial for both parties. Thirdly, recognizing and promoting ADR will significantly decrease the number of cases brought in front of courts. This scope of application of this regulation will impact a huge number of entities and establishments all over the world with the main victims being small and medium-sized businesses. Thus, the number of low or medium-value cases against these types of establishments will overwhelm judicial courts. Fourthly, if recognition is still a far-off concept, the GDPR should at least assign specific DPAs for arbitration. Accordingly, it will be better organized, create consistency in application, and avoid

unnecessary mistakes that may result from not knowing or not fully understanding the rights, obligations, or enforcement mechanisms of the GDPR.

- From the ADR's perspective, flexibility and other characteristics of extra-judicial dispute resolutions processes are double-edged. Accordingly, they can be misused by parties or disputants under the pretense of data protection and privacy to strategically hide information, or use data in a way that may unnecessarily elongate the process. Thus, it is important to have clear guidelines and laws that forbid the utilization of data protection laws in this sense.

- ADR mechanisms other than arbitration will become less used in the context of data protection and privacy disputes. The reason behind that is the lack of worldwide enforcement capabilities of their awards. This will render concepts like the "Best Alternative to a Negotiated Agreement" (BATNA) and "Worst Alternative to a Negotiated Agreement" (WATNA) as futile. As it stands, stakeholders will need to balance the value of dispute resolution methods (mediation and negotiation) as a function of their speed, efficiency, and commercial and personal interests rather than considering their legal rights since they can't guarantee enforcement. Thus, with no formal worldwide enforcement of these methods, the value of other extra-judicial dispute resolution processes will lose value based on the principle of economic utility, since they will need to invest resources in securing a court judgment that will most probably be of international status. Therefore, the best way forward is to work on increasing the enforcement power of these mechanisms to preserve their value and usage, especially in the transnational context of data protection and privacy regulations. Hence, for the time being, arbitration will remain to be the go extra-judicial dispute resolution process, since it is backed by the New-York convention and guarantees worldwide enforcement.

- Building on the previous recommendations, the regulation of data protection should be handled by international communities. The only way to achieve data protection in a borderless world is to do so collectively via international efforts and not impose a national regulation internationally. Additionally, efforts from both the regulators of these laws and the extra-judicial dispute resolution

communities should work together to balance the proper utilization of these mechanisms in a way that improves enforcement and guarantee the protection of the right to privacy and data protection.

2- Concerning Cybersecurity and ADR

- The main issue with cyberspace is that no one has complete and total control over its borderless and digital nature. Accordingly, threats from the digital world can't be completely stopped or permanently eliminated. Thus, regulators and international communities should approach this subject from a different perspective than the one used to deal with physical crimes of the natural world. Hence, the need for remedies, not solutions is necessary. Therefore, the focus must shift from spending huge amounts of money on firewall systems and trying to build a digital fortress, to investing in building and achieving total cyber-awareness among people building awareness can go from simple training sessions, constant reminders, frequent television or radio advertisements and shows on these subjects, to enforcing regulations and applying fines to those who don't follow cybersecurity principles. This subject could be approached the same way that COVID-19 was approached in regards to issuing fines for breaches of social distancing rules, mandatory mask-wearing, opening after curfew hours, etc. We must try to control what can be controlled because securing the weak link (i.e., humans) is the most important aspect in thwarting off cyberthreats.

- There should be a proactive approach rather than a reactive one. This idea could be implemented in a form of a feedback or accreditation system for companies and establishments. For example, an application, software, or online database system could be created that serves the purpose of giving off ratings for the security of each company. It could be done through user feedback and reviews, the input of specialists who conduct period visits, and a statistical format that shows a company's susceptibility to breaches and if it had suffered one or several breaches in the past. This is just like the "Uber Taxi" review system or the one used for restaurants and markets to tell consumers about the overall quality of the experience to be expected. It could also resemble the format used when creating a password which shows the strength of a password as "weak/ medium/ strong" depending on the combinations used or the "star rating system". The proposed accreditation system will show the strength of the security system of the company as a direct pop-up when entering its website or the specific app used for this purpose. Accordingly, it will limit entering into transactions with establishments that have bad reviews or ratings concerning their

digital security. Of course, there will be a filtration system within the application that removes spam reviews or those which play no role other than to ruin an establishment's reputation. Consequently, this will prevent disputes from even happening and force these companies to modify their systems, since the monetary system we live in will force them to either adapt or close up for not making profits. In turn, this will also benefit judicial and extra-judicial systems, because of the decrease in the number of cases.

- The ICCA-NYC Bar-CPR Protocol on Cybersecurity in international arbitration should be codified and attain the status and power of a legally binding law. This step is necessary to ensure that parties, arbitrators, and institutions abide by cybersecurity measures that would have liability clauses in case of breaching its principles. The problem in the current use of the protocol is that there are no accountability and liability principles for not abiding by cybersecurity principles. The only basis for accountability is found in the duties of arbitrators as discussed, since thwarting off cyber-intrusions is a natural extension of his traditional duties as an arbitrator. Thus, promoting the protocol to a law status would establish a clear set of principles and rules to be followed by the involved parties, the lack of which will raise liability concerns.

- There should be a clear and explicit law or procedure that addresses the duty of arbitrators to avoid cybersecurity breaches, and the admissibility and use of evidence obtained through cyber-breaches. This recommendation directly feeds into the previous one. The lack of a clear and explicit set of rules as established in the thesis would result in several interpretations of traditional concepts that may or may not apply in the context of the cyberworld. Thus, rather than applying the laws of the actual world on cyberspace and trying to figure out which traditional law can be expanded and interpreted in a way that covers cyberspace, why not set an explicit law that eliminates interpretations and directly governs the issues of the virtual world concerning arbitration.

3- Concerning ODR

- The New York Convention should be amended to include the digital formats of today's world. It isn't acceptable to debate and persist on interpreting and widening the scope of a convention that was established almost 50 years before the widespread of technology and its tools. New mechanisms need new regulations to fully appreciate them.

- Decisions in arbitration and online arbitration should be published. Publishing can be achieved by preserving confidentiality through redacting certain names or places or other indications that point to the parties involved. The purpose of such a recommendation is to build trust and transparency in the process and establish consistency. Thus, creating precedents that would help facilitate decision making and the efficiency of the process. It would also encourage parties to select this route rather than judicial methods.

- The new type of borderless disputes in e-commerce that are mostly of low and medium value should be prevented and not solved. In other words, the focus must shift from constantly trying to modify traditional ADR methods by adding new rules and guidelines and trying to apply them in the context of ODR on e-disputes, to utilizing Online Dispute Prevention Resolutions (ODPR). The importance of ODPR is magnified in the digital world. Being able to prevent most low and medium-value e-commerce and other disputes that happen in cyberspace will result in a massive overhaul in the extra-judicial and judicial systems. To achieve this goal, the role of online mediation and online negotiation must increase dramatically. These mechanisms should be equipped with the proper tools needed to actually prevent disputes, rather than elongating the time in which the parties go back to arbitrations or resort to normal judicial methods. It could be achieved through the backing of international communities that can increase the effectiveness of the role of mediators by giving them powers to force a change in opinions and close gaps in perspectives.

- Following the previous recommendation, multi-method dispute resolution processes must become the norm in ODR. It may be better to combine the three processes rather than wasting time and money going from one to another. It could be perceived as an elevator in the same building rather than three different buildings. It would force parties to go through the levels in order to solve their dispute. Thus, increasing the dependency on negotiation and mediation. Hence, increasing the rate of solvable disputes before reaching arbitration or litigation, and without the complexities of moving from one method to another. Moreover, this recommendation fits in perfectly with the notion of ODPR, since most of the time parties aren’t aware that their disputes can be mitigated

through negotiation and mediation, so forcing them to go through these stages could benefit everyone involved.

4- Concerning AI

- This field needs to be perceived as and dealt with in a different manner than the one administered to handle IT integration in the judicial and extra-judicial systems. Traditional concepts and broad interpretations of conventional principles, rules, and regulations won’t be enough. It remains to be seen how AI integration and their potential takeover would create a new system of dispute resolution. Hence, the debate about preserving the specificity of traditional ADR methods will be a quarrel of the past.

BIBIOLOGRAPHY

I- Traditional References:

A- Books

1- Abdel Wahab (Mohamad S.), Katsh (Ethan) & Rainey (Daniel), **Online Dispute Resolution: Theory and Practice**, Eleven International Publishing, The Hague, Netherlands, February 2013

2- Albrecht (Jan P.), Jotzo (Florian), **Das Neue Datenschutzrecht Der EU, "The EU's New Data Protection Law"**, published by Nomos, Germany, 2017

3- Barrett (Jerome T.), Barrett (Joseph P.), **A History of Alternative Dispute Resolution: The Story of a Political, Cultural and Social Movement**, published in Affiliation with The Association For Conflict Resolution, August, 2004

4- Born (Gary B.), **International Commercial Arbitration (A Three-Volume Book Set), Second Edition, Volume II: International Arbitration Procedures and Proceedings**, published by Wolters Kluwer Law & Business; 2nd edition, The Netherlands, April 22, 2014

5- Cortes (Pablo), **Online Dispute Resolution for Consumers in the European Union**, published by Routledge Research in IT and E-Commerce Law, London and New York, 2011

6- Haley-Nolan (Jacqueline), **Alternative Dispute Resolution in a Nutshell**, West Academic Publishing, 4th Edition, Minnesota, USA, 2013

7- Hörnle (Julia), **Cross-Border Internet Dispute Resolution**, Cambridge University Press, New York, USA, February, 2009

8- Katsh (Ethan), Rifkin (Janet), **Online Dispute Resolution: Resolving Conflicts in Cyberspace**, San-Francisco: Jossey-Bass, USA, May, 2001

9- Kaufmann- Kohler (Gabrielle), Schultz (Thomas), **Online Dispute Resolution: Challenges for Contemporary Justice**, Published in Kluwer Law International: The Hague, Zurich, 2004

10- Kissinger (Henry), **World Order**, published by the Penguin Group, New York, USA, 2014

11- Rule (Colin), **Online Dispute Resolution For Business: B2B, E-Commerce, Consumer, Employment, Insurance, and other Commercial Conflicts**, John Wiley & Sons, September, 2002

12- Raul (Alan C.), Fairloth (Frances E.), Mohen (Vivek K.), **The Privacy, Data Protection and Cybersecurity Law Review**, edited by Alan Charles Raul, published by Gideo Roberton, Fourth Edition, UK, Business Research LTD London, December, 2017

13- Shinder (Debra L.), **Scene of the Cybercrime, Computer Forensics Handbook**, published by Syngress Publishing, Inc., USA, 2002

14- Tweeddale (Andrew), Tweeddale (Keren), **Arbitration of Commercial Disputes, International and English Law and Practice**, published by Oxford University Press, England, Oxford, 2005

15- Voigt (Paul), Bussche (Axel von dem), **The EU General Data Protection Regulation (GDPR): A Practical Guide**, Springer International Publishing, 2017

16- Wang F. (Fangfei), **Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective**, Chandos Series on Publishing, 1st Edition, Oxford England, 2009

17- Zuboff (Shoshana), **The Age of Surveillance Capitalism**, first published by Profile Books Ltd, 1st Edition, London, 2019

B- Articles

1- Roebuck (Derek), **Cleopatra Compromised: Arbitration in Egypt in the First Century BC**, Journal of the Chartered Institute of Arbitrators, Volume 74, Issue 3, August, 2008, pp. 263-268

2- Kreis (Falco), Kaulartz (Markus), **Smart Contracts and Dispute Resolution- A Chance to Raise Efficiency?** ASA Bulletin, Volume 37, Issue 2, June, 2019

3- Mathews (Robert), **Interrogation "privacy" in a world brimming with high political entanglements, surveillance, interdependence & interconnections**, published in "Health and Technology", Issue 7, 2017, pp. 265- 324

4- Shwartz (Paul. M), **Privacy Inalienability and the Regulation of Spyware**, published in Berkeley Technology Law Journal, Vol. 20, 2005, pp. 1269-1282

5- Shwartz (Paul. M), **Property, Privacy, and Personal Data**, published in Harvard Law Review, Vol. 117 Review 2055, 2003-2004, pp. 2056-2125

C- Case Laws

a) International Courts- Arbitration Judgments

1- ICISID Case No. ARB/06/8, International Centre for Settlement of Investment Disputes, Libananco Holdings Co. Limited v. Republic of Turkey, May 22, 2013

2- ICSID Case No. ARB/13/13, International Centre for Settlement of Investment Disputes, Caratube International Oil Company LLP and Mr. Devincci Salah Hourani v. Republic of Kazakhstan, September 27, 2017

3- ICSID Case No. ARB/07/30, ConocoPhillips Petrozuata B.V., ConocoPhillips Hamaca B.V. and ConocoPhillips Gulf of Paria B.V. v. Bolivarian Republic of Venezuela, 2019

4- PCA Case No. AA 227, In the Matter of an Arbitration Before a Tribunal Constituted in Accordance with Article 26 of the Energy Charter Treaty and The 1976 UNCITRAL Arbitration Rules, between Yukos Universal Limited (Isle of Man) and The Russian Federation, July 18, 2014

5- PCA Case No. AA 226, In the Matter of an Arbitration Before a Tribunal Constituted in Accordance with Article 26 of the Energy Charter Treaty and The 1976 UNCITRAL Arbitration Rules, between Hulley Enterprises Limited (Cyprus) and The Russian Federation, July 18, 2014

b) European Union Cases and Court Judgments

1- CJEU (Grand Chamber), Case C-362/14, Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd, October 6, 2015

2- CJEU (Grand Chamber) Case C-131/12 Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, May 13, 2014

3- CJEU (Grand Chamber), Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, 16 July, 2020

4- CJEU (Third Chamber), Case C-230/14, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, October 1, 2015

c) Ireland Cases

1- The High Court of Ireland Judicial Review, Case No. 765JR/2013, between Maximillian Schrems and Data Protection Commissioner, June 18, 2014

d) France Cases and Committee Decisions

1- The Council of State (Conseil D'État), CR litigation, No. 430810, GOOGLE LLC COMPANY, Session of June 12, 2020, Reading of June 19, 2020

2- French Court of Cassation (First Civil Chamber), (Cass, 1ère civ), Société Procédés de Préfabrication pour le béton v. Libye, October 28, 1977, published in *Revue de l'arbitrage* (no. 2, 1998), pp. 399-407

3- Deliberation of the Restricted Committee of the CNIL, SAN-2019-001 of January 21, 2017, pronouncing a financial sanction against GOOGLE LLC

4- Deliberation of the Restricted Committee of the CNIL, SAN-2020-012 of December 7, 2020, concerning the companies GOOGLE LLC and GOOGLE IRELAND LIMITED

5- Deliberation of the Restricted Committee of the CNIL, SAN-2020-013 of December 7, 2020, concerning the company AMAZON EUROPE CORE

e) United Kingdom Case

1- Entick v. Carrington (1765) 19 St. Tr. 1030

f) United States of America Cases

1- United States District Court, D. - Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902)

2- United States Supreme Court of Georgia, Pavesich v. New England Life Ins. Co., 122 Ga. 190 (Ga. 1905)

3- United States Supreme Court, Cox Broadcasting Corp. v. Cohn, No. 73-938, 420 U.S. 469 (1975)

4- United States District Court, D. Delaware, Victoria del la Mata v. American Life Insurance Company- "Civ. A. No. 90-173 MMS- 771 F.Supp. 1375" (1991)

5- United States District Court for the District of Columbia, Vladimir Matusevitch v. Vladimir Ivanovich Telnikoff, - "Civ. A. No. 94-1151 RMU – 877 F. Supp.1" (1995)

6- United States Court of Appeals For the Ninth Circuit of California, Cindy Lee Garcia v. Google, Inc, No. 12-57302, (2015)

7- United States District Court of the Southern District of New York, Rahul Manchanda v. Google, Inc, et al, No.1:16-CV-3550 (JPO), (S.D.N.Y. 2016)

D- Laws and Legislations[132]

a) International Conventions

1- The OECD Privacy Guidelines, 2011

b) European Union Legislations

1- Treaty on the Functioning of the European Union, 1957

2- 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

[132] Laws and Legislations are ordered according to chronological order in each section

movement of such data, Official Journal of the European Communities, No L 281/31, 23/11/1995

3- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market “Directive on electronic commerce”, published in the Official Journal of the European Communities, L 178, 17/7/2000

4- Commission Decision 2000/520/EC, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, published in the Official Journal of the European Communities, L 215, 25/8/2000

5- Charter of Fundamental Rights of the European Union, published in the Official Journal of the European Communities, C 364/1, 18/12/2000

6- Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM/2013/0847 final, November 27, 2013

7- European Convention on Human Rights, Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), Strasbourg, 2013

8- Regulation (EU) 2016/679 of the European Parliament and 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- The General Data Protection Regulation (GDPR), Official Journal of the European Union, No. L 119/1, 4/5/2016

9- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 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, published in the Official Journal of the European Union, C 4176, 1/9/2016

10- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, published in the Official Journal of the European Union, L 303/59, 28/11/2018

c) United Kingdom Legislations

1- Justices of the Peace Act- 1361 (34 Edw 31c 1)

2- UK Arbitration Act of 1996

3- Irish Data Protection Bill (No. 10b of 2018)

d) Switzerland Legislation

1-Switzerland's Federal Code on Private International Law (CPIL) of December 18, 1987, went into effect January 1st, 2017

e) United States of America Legislations

1- Privacy Act of 1974, Pub. L. No 93-579, 88 Stat. 1896 (Dec. 31, 1974), codified at 5 U.S.C. §552a (1974)

2- Restatement (Third) of Foreign Relations Law of the United States, 1988

3- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, (USA PATRIOT ACT) ACT OF 2001, Pub. L. No 107-56, 115 Stat. 272 (Oct. 26, 2001)

5- The White House, Policy Directive/ PPD-28, January 17, 2014

4- Uniting and Strengthening America By Fulfilling Rights and Ensuring Effective Discipline Over Monitoring, Act of 2015, Pub L. 114-23, 129 Stat. 268 (June 2, 2015)

6- 114th Congress of the United States of America, USA FREEDOM Act, H.R. 2048, Pub. L 114-24 (2015)

7- 114th Congress of the United States of America, Judicial Redress Act of 2015, Pub. L 114-126 (Feb. 24,2016)

f) Arbitration Conventions, Laws, Rules, and Protocols

1- United Nations Conference on International Commercial Arbitration, Convention on the Recognition and Enforcement of Foreign Arbitral Awards, United Nations, 1958, “The New-York Convention”

2- UNCITRAL Model Law on International Commercial Arbitration, 1985

3- IBA Rules of Ethics for International Arbitrators, 1987

4- ABA/AAA Code of Ethics for Arbitrators in Commercial Disputes, March 1, 2004

5- International Bar Association (IBA) Rules on the Taking of Evidence in International Arbitration, 2010

6- International Dispute Resolution Procedures (ICDR) Rules, June 1, 2014

7- London Court of International Arbitration (LCIA) Arbitration Rules (2014)

8- ICCA-IBA Joint Task Force on Data Protection in International Arbitration, Roadmap to Data Protection in International Arbitration, Draft Protocol, February 28, 2019

9- The ICCA Report No.6: ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration, 2020 Edition

10- International Chamber of Commerce (ICC), 2021 Arbitration Rules

E- Encyclopedia and Dictionary

1- West's Encyclopedia of American Law, Ed. 2, 2008

2- Collins Dictionary of Law, Ed. 3, 2006

II- Electronic References:

A- Online Books

1- ICC, **Cybersecurity Guide for Business**, 2015, found at https://www.iccwbo.be/wp-content/uploads/2016/05/ICC-Cyber-security-guide-for-business.pdf visitation date 8/1/2021

2- Privacy International, **A Guide for Policy Engagement on Data Protection**, **Part 1: Data Protection Explained**, published September 2018, found at https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf visitation date 1/2/2020

3- Simpli Learn**, An Introduction to Cyber Security: A beginner's Guide**, last updated August 24, 2020, found at https://www.simplilearn.com/introduction-to-cyber-security-beginners-guide-pdf visitation date 17/12/2020

B- Online Academic Articles

1- Ackerman (Susan-Rose), **Inalienability and the Theory of Property Rights**, published in Columbia Law Review, Vol. 85, Number 5, June 1985, pp. 931-969, found at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1592&context=fss_papers visitation date 20/5/2021

2- Albrecht (Jan P.), **How the GDPR Will Change the World**, published in EDPL, March 2016, pp. 287-289, found at https://edpl.lexxion.eu/data/article/10073/pdf/edpl_2016_03-005.pdf visitation date 5/4/2021

3- Benyekhlef (Karim), Gelinas (Fabien), **Online Dispute Resolution**, Lex Electronica, Volume 10, No. 2, 2005, found at https://www.lex-electronica.org/files/sites/103/10-2_benyekhlef-gelinas.pdf visitation date 12/5/2021

4- Blair (Cherie), Gojkovic (Ema V.), **WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence**, published in ICSID Review: Foreign Investment Law Journal, Volume 33, Issue No. 1, February 3, 2018, pp. 235-259, found

at https://omniastrategy.com/wp-content/uploads/WikiLeaks-and-Beyond.pdf visitation date 4/1/2020

5- Brandies (Louis), Warren (Samuel), **The Right to Privacy**, Harvard Law Review, Volume 4, Issue 5, December 15, 1890, pp. 193-220, found at https://www.jstor.org/stable/i256795 visitation date 25/3/2020

6- Buxbaum (Hannah L.), **Territory, Territoriality, and the Resolution of Jurisdictional Conflict**, Maurer Faculty, published in The American Journal of Comparative Law, Volume 57, 2009, pp. 631-675, found at https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1132&context=facpub visitation date 15/4/2021

7- Cohen (Stephanie), Morril (Mark), **A Call To Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion**, published in The Fordham International Law Journal, Volume 40, Issue 3, 2017, pp. 982-1012, found at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2657&context=ilj visitation date 6/1/2021

8- Cooper (Daniel), Tielemans (Henriette), Fink (David), **The Lisbon Treaty and data protection: What's next for Europe's privacy rules?** Published in the Privacy Advisor-International Association of Privacy Professionals, January- February 2010, pp.17-18, found at https://www.cov.com/en/news-and-insights/insights/2010/02/the-lisbon-treaty-and-data-protection-whats-next-for-europes-privacy-rules visitation date 5/10/2020

9- Eisen (Joel B.), **Are We Ready for Mediation in Cyberspace?** Published in Brigham Young University Law Review, Volume 4, 1998, pp. 1305-1360, found at https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=2824&context=lawreview visitation date 25/4/2021

10- Galanter (Marc), **The Day After the Litigation Explosion**, Maryland Law Review, Volume 46, Number 3, Issue 1, 1986, found at https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2633&context=mlr visitation date 14/2/2020

11- Hert (Paul de), Czerniawski (Michal), **Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context**, published in International Data Privacy Law, Volume 6, Issue 3, August 2016, pp. 230-243, found at https://academic.oup.com/idpl/article/6/3/230/2447252?login=true visitation date 15/4/2021

12- Hill (Richard), **Online Arbitration: issues and solutions**, published in Arbitration International, Volume 15, Issue 2, June 1, 1999, pp. 199-207, found at http://www.umass.edu/dispute/hill.htm visitation date 25/4/2021

13- Holvast (Jan), **History of Privacy**, Part of a book by Matyáš (Vashek) et al. (Eds.): **The Future of Identity**, IFIP AICT 298, published by Springer Nature, Switzerland, pp. 13-42, 2009, found at https://link.springer.com/content/pdf/10.1007%2F978-3-642-03315-5_2.pdf visitation date 15/5/2020

14- Hustinx (Peter), **Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation**, found at: https://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf visitation date 15/1/2020

15- Heuvel (Esther van den), **Online Dispute Resolution as a Solution to Cross-Border E-Disputes: An Introduction to ODR**, 1997, found at http://www.oecd.org/internet/consumer/1878940.pdf visitation date 19/4/2021

16- Janićijević (Dejan), **Delocalization of International Commercial Arbitration**, published in Facta Universitatis, Law and Politics, Volume 3, Number 1, 2005, pp. 63-71, found at http://facta.junis.ni.ac.rs/lap/lap2005/lap2005-07.pdf visitation date 19/4/2021

17- Maldoff (Gabe), Tane (Omar), **Privacy Shield Backgrounder,** excerpt taken from **"Essential Equivalence and European Adequacy after Schrems: The Canadian Example"**. Published in Wisconsin International Law Journal, Volume 34, 2016, found at https://iapp.org/resources/article/privacy-shield-backgrounder/ visitation date 10/6/2020

18- Myers (Anna), CIPP/US, IAPP Westin Fellow**, FTC Enforcement of the U.S.-EU Safe Harbor Framework**, no publication date, found at

https://iapp.org/media/pdf/resource_center/IAPP_FTC_SH-enforcement.pdf visitation date: 13/6/2020

19- Paisley (Kathleen), **It's All About the Data: The Impact of the EU General Data Protection Regulation on International Arbitration**, published in Fordham International Law Journal, Volume 41, Issue 4, 2018, pp. 841-931, found at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2707&context=ilj visitation date 9/12/2020

20- Pastore (Jim), **Practical Approaches to Cybersecurity in Arbitration**, Fordham Law Journal, Volume 40, Issue 3, 2017, pp. 1022-1032, found at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2658&context=ilj visitation date 8/1/2020

21- Reding (Viviane), **The Debate on Privacy and Security Over the Network: Regulation and Markets**, published by Ariel and Fundación Telefónica, Volume 36, printed in Spain October 2012, Executive Summary pp 13-14, Found at https://lirias.kuleuven.be/retrieve/226688 visitation date 12/2/2020

22- Rosenthal (David), **Complying with the General Data Protection Regulation (GDPR) in International Arbitration- Practical Guidance**, Journal in 37 ASA Bull. 4/2019, published by Kluwer Law International, The Netherlands, pp. 822-852, found at https://www.rosenthal.ch/downloads/Rosenthal-ArbitrationGDRP.pdf visitation date 11/12/2020

23- Scherer (Maxi), **Artificial Intelligence and Legal Decision-Making: The Wide Open? A Study Examining International Arbitration**, published in the Journal of International Arbitration, Volume 36, Number 5, 2019, pp. 539-574, found at https://3rdsifocc.tpi.sg/assets/documents/SCHERER%20Artificial%20Intelligence%20and%20Legal%20Decision-Making[7].pdf visitation date 5/1/2021

24- Schmitz (Amy. J), **'Drive-Thru' Arbitration in the Digital Age: Empowering Consumers Through Binding ODR**, Baylor Law Review, Volume 62, Issue 1, 2010, pp. 178-244, found at https://core.ac.uk/download/pdf/217048178.pdf visitation date 15/2/2020

25- Schwartz (Paul. M), Peifer (Karl- Nikolaus), **Transatlantic Data Privacy Law**, published in Georgetown Law Journal, Volume 106:115, 2017, pp. 115-179, found at https://escholarship.org/content/qt1ws1r1cz/qt1ws1r1cz_noSplash_816c6e2b4eaaaec14b0a03ecedd4031b.pdf?t=p68tx6 visitation date 6/4/2020

26- Shah (Aashit), **Using ADR to Solve Online Disputes**, published in Richmond Journal of Law & Technology, Volume 10, Issue 3, 2004, found at https://jolt.richmond.edu/jolt-archive/v10i3/article25.pdf visitation date 15/4/2021

27- Sinha (G. Alex), **NSA Surveillance since 9/11 and the Human Right to Privacy**, Loyola Law Review, Volume 59, 2012-2013, pp. 861-946, found at https://dspace.loyno.edu/jspui/bitstream/123456789/121/1/Sinha.pdf visitation date 18/5/2020

28- Tourkochoriti (Ioanna), **The Transatlantic Flow of Data and the National Security Exception in the European Privacy Regulation: In Search For Legal Protection Against Surveillance**, published by Penn Law: Legal Scholarship Repository, Volume 36:2, 2015, pp. 459-524, found at https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1891&context=jil visitation date 13/6/2020

29- Victorio (Richard M.), **Internet Dispute Resolution (iDR): Bringing ADR into the 21st Century**, published in Pepperdine Dispute Resolution Law Journal, Volume 1: 279, 2001, pp.279-300, found at https://law.pepperdine.edu/dispute-resolution-law-journal/issues/volume-one/15-victorio.pdf visitation date 15/4/2021

30- Werra (Jacques de), **Using Arbitration and ADR for Disputes About Personal and Non-Personal Data: What Lessons From Recent Developments in Europe**, published in the American Review of International Arbitration (ARIA), Vol. 3, No.2 © JurisNet, LLC, 2019, pp. 195-217, found at https://www.digitallawcenter.ch/sites/default/files/publications/unige_134313_attachment01.pdf visitation date 12/12/2020

B- Online Thesis

1- Manevy (Isabelle), **Online Dispute Resolution: what future?** D.E.A de droit anglaise et nord-americian des affaires, University de Paris 1, June 2001, found at http://lthoumyre.chez.com/uni/mem/17/odr01.pdf visitation date 18/4/2021

C- Online Surveys, Reports and Guides

1- Article 29 Data Protection Working Party, 00339/09/EN, WP 158, **Working Document 1/2009 on pre-trial discovery for cross border civil litigation**, adopted on 11 February 2009, found at https://www.gpdp.gov.mo/uploadfile/others/wp158_en.pdf visitation date 13/12/2020

2- Chartered Institute of Arbitrators (CIArb), **CIArb Costs of International Arbitration Survey 2011**, found at https://www.iaa-network.com/wp-content/uploads/2017/01/CIArb-Cost-of-International-Arbitration-Survey.pdf visitation date 18/4/2021

3- European Commission, Van Eecke (Patrick), Maarten (Truyens), **EU Study on the Legal analysis of a single market for the Information Society: New rules for a new age?** November 2009, published by DLA Piper UK LLP, July 22, 2014, found at https://op.europa.eu/en/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722# visitation date 15/4/2021

4- European Committee on Legal Co-operation (CDCJ), **Technical Study on Online Dispute Resolution Mechanisms**, CDCJ (2018) 5, Strasbourg, August 1, 2018, found at https://rm.coe.int/cdcj-technical-study-on-online-dispute-resolution-mechanisms/16809f0079 visitation date 18/4/2021

5- **How will artificial intelligence affect the legal profession in the next decade**, Debate under Queen's Law Reports, November 3, 2015, found at https://law.queensu.ca/news/how-will-artificial-intelligence-affect-the-legal-profession-in-the-next-decade visitation date 19/5/2021

6- The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition), January 2017, found at https://thesedonaconference.org/sites/default/files/publications/International%2520Litigation%2520Principles_Transitional%2520Ed_Jan%25202017.pdf visitation date 12/12/2020

7- The Seoul Protocol on Videoconferencing, found at http://www.sidrc.org/static_root/userUpload/data/[FINAL]%20Seoul%20Protocol%20on%20Video%20Conference%20in%20International%20Arbitration.pdf visitation date 10/1/2020

8- UNCITRAL Notes on Organizing Arbitral Proceedings, New York, 2016, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/arb-notes-2016-e.pdf visitation date 6/1/2021

D- Other Online Sources

a) Online Seminar

1- CIArb Singapore "Cybersecurity and Data Protection Webinar", with Kathleen Paisley as a Speaker, Virtual seminar held on Zoom, November 24, 2020

b) Press Releases

2- **Equifax Announces Cybersecurity Incident Involving Consumer Information**, press release, found at https://investor.equifax.com/news-and-events/press-releases/2017/09-07-2017-213000628 visitation date 29/12/2020

3- Federal Trade Commission, **FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy**, August 29, 2013, found at https://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers visitation date 18/10/2020

4- Federal Trade Commission, **FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook**, July 24, 2019, found at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions visitation date 18/10/2020

5- Federal Trade Commission, **FTC Sues Cambridge Analytic, Settles with Former CEO and App Developer**, July 24, 2019, found at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer visitation date 18/10/2020

c) Official Newspapers

1- Bowcott (Owen), **'Right to be forgotten' could threaten global free speech, says NGOs,** published in The Guardian, September 9, 2018, found at https://www.theguardian.com/technology/2018/sep/09/right-to-be-forgotten-could-threaten-global-free-speech-say-ngos visitation date 25/8/2020

2- Confessore (Nicholas), Cambridge Analytica and Facebook**: The Scandal and the Fallout So Far**, published in The New York Times, April 4, 2018, found at https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html visitation date 4/4/2021

3- Greenwald (Glenn), MacAskill (Ewen), **NSA Prism program taps into user data of Apple, Google and others**, published in The Guardian, June 7, 2013, found at https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data visitation date 18/5/2020

4- Levine (Robert), **Behind the European Privacy Ruling That's Confounding Silicon Valley**, published in The New-York Times, October 9, 2015, found at https://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html visitation date 15/6/2020

5- Macaskill (Ewen), Dance (Gabriel), **NSA Files: Decoded- What the revelations mean for you**, published in The Guardian, November 1, 2013, , found at https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 visitation date 18/5/2020

6- Noyes (Katherine), Deloitte, **Privacy Shield is Dead. Now What?** Published in The Wall Street Journal, September 11, 2020, found at

https://deloitte.wsj.com/riskandcompliance/2020/09/11/privacy-shield-is-dead-now-what/ visitation date 15/10/2020

d) Online Blogs and Writings

1- Analytics Insight, **Data Protection vs. Cybersecurity: Why You Need Both**, August 29, 2020, found at https://www.analyticsinsight.net/data-protection-vs-cyber-security-why-you-need-both/ visitation date 17/12/2020

2- Baxter (Michael), **GDPR anniversary: has the regulation backfired? What next?** published March 27, 2019, found at https://www.information-age.com/gdpr-anniversary-citizens-custodians-of-data-privacy-by-design-trust-by-design-123482779/ visitation date 29/8/2020

3- Bernstein (Danielle), **Why the "Right to be Forgotten Won't Make it to the United States**, published in Michigan Technology Law Review, February 2020, found at http://mttlr.org/2020/02/why-the-right-to-be-forgotten-wont-make-it-to-the-united-states/ visitation date 29/8/2020

4- Cave (Bryan), **A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor"**, June 16, 2019, found at https://iapp.org/media/pdf/resource_center/Comparison-of-Privacy-Shield-and-the-Safe-Harbor.pdf visitation date 16/6/2020

5- Chauhan (Aditya S.), **Future of AI in Arbitration: The Fine Line Between Fiction and Reality**, published in Kluwer Arbitration Blog, September 26, 2020, found at http://arbitrationblog.kluwerarbitration.com/2020/09/26/future-of-ai-in-arbitration-the-fine-line-between-fiction-and-reality/ visitation date 19/4/2021

6- Chen (Caleb), **The head of Denmark's spy program has been fired for snooping on citizens and lying about it**, published on Privacy news online, August 26, 2020, found at https://www.privateinternetaccess.com/blog/the-head-of-denmarks-spy-program-has-been-fired-for-snooping-on-citizens-and-lying-about-it/ visitation date 10/10/2020

7- Cisco, **What is Information Security?** No publication date, found at https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html visitation date 17/12//2020

8- Cole (Tony), **The Seoul Protocol on Videoconferencing and the Coronavirus (COVID-19) Pandemic**, May 19, 2020, found at https://www.lexology.com/library/detail.aspx?g=577b26b4-5372-4bc4-afba-ad72e60a94ba visitation date 10/1/2020

9- Cottle (Giles), **A year of GDPR: blocked users, hot potato, and opt-in fatigue**, published June 18, 2019, found at https://deductive.com/blogs/year-gdpr-blocked-users-hot-potato-opt-in-fatigure/ visitation date 29/8/2020

10- Electronic Privacy Information Center, "**EU Privacy and Electronic Communications (e-Privacy Directive)**", found at https://epic.org/international/eu_privacy_and_electronic_comm.html visitation date 5/2/2020

11- Electronic Privacy Information Center, **The Lisbon Treaty and Privacy**, no publication date, found at https://epic.org/privacy/intl/lisbon_treaty.html#:~:text=Under%20the%20Lisbon%20Treaty%2C%20the,recognized%20as%20a%20fundamental%20right.&text=%22As%20a%20consequence%2C%22%20he,by%20individuals%20is%20not%20unlimited. visitation date 5/10/2020

12- Frankenfield (Jake), **Predictive Modeling**, published in Investopedia, last updated June 27, 2019, found at https://www.investopedia.com/terms/p/predictive-modeling.asp visitation date 19/4/2021

13- Frankenfield (Jake), **Artificial Neural Network**, published in Investopedia, last updated August 28, 2020, found at https://www.investopedia.com/terms/a/artificial-neural-networks-ann.asp#:~:text=An%20artificial%20neural%20network%20(ANN)%20is%20the%20piece%20of%20a,by%20human%20or%20statistical%20standards visitation date 19/5/2021

14- Greene (David**), European Court's Decision in Right To Be Forgotten Case is a Win for Free Speech**, Deeplinks Blog, published September 26, 2019, found at https://www.eff.org/deeplinks/2019/09/european-courts-decision-right-be-forgotten-case-win-free-s#:~:text=In%20a%20significant%20victory%20for,by%20users%20around%20the%20world. visitation date 29/8/2020

15- Herbert Smith Freehills Arbitration Notes, Update [6]: **"Necessity is the Mother of Invention": Covid-19 Dramatically Accelerates Digitalization of Arbitration Processes**, June 12, 2020, found at https://hsfnotes.com/arbitration/wp-content/uploads/sites/4/2020/06/COVID-19-Responses-of-Institutions-and-Organisations-11-June-2020-HSF-Arbitration-Notes.pdf visitation date 10/1/2021

16- Johnson (Joseph), Worldwide digital population as of January 2021, Statista, published April 7, 2021, found at https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=As%20of%20January%202021%20there,the%20internet%20via%20mobile%20devices visitation date 7/5/2021

17- Khosrowshahi (Dara), **2016 Data Security Incident**, November 21, 2017, Uber Official Website, found at Uber's official website: https://www.uber.com/newsroom/2016-data-incident/ visitation date 29/12/2020

18- King (Lawrence), **Why Cybersecurity Education for Employees is so important**, July 30, 2019, found at https://www.cyberdefensemagazine.com/end-user-security-education/ visitation date 17/12/2020

19- Kloth (Alexander), **One Law to Rule the all, On the extraterritorial applicability of the new EU General Data Protection Regulation**, published on Volkerrechtsblog, February 5, 2018, found at https://voelkerrechtsblog.org/one-law-to-rule-them-all/ visitation date 4/4/2021

20- Layton (Roslyn), **The 10 Problems of the GDPR, Testimony**, published by the American Enterprise Institute, March 12, 2019, found at https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf visitation date 25/8/2020

21- Leetaru (Kalev), **Will the EU's Data Protection Act Actually Lead to Less Online Privacy?** published May 8, 2018, found at https://www.forbes.com/sites/kalevleetaru/2018/05/08/will-the-eus-data-protection-act-actually-lead-to-less-online-privacy/?sh=678605cf355a visitation date 30/8/2020

22- Lessing (Marlese), **Case Study: WannaCry Ransomware**, July 9, 2020, found at https://www.sdxcentral.com/security/definitions/case-study-wannacry-ransomware/ visitation date 29/12/2020

23- Loebl (Zbynek), **Can a robojudge be fair**, published in Kluwer Arbitration Blog, December 16, 2019, found at http://arbitrationblog.kluwerarbitration.com/2019/12/16/can-a-robojudge-be-fair/ visitation date 19/5/2021

24- Lomas (Natasha), **Most EU cookie 'consent' notices are meaningless or manipulative, study finds**, published on Tech- Crunch, August 10, 2019, found at https://techcrunch.com/2019/08/10/most-eu-cookie-consent-notices-are-meaningless-or-manipulative-study-finds/ visitation date 29/8/2020

25- Masnick (Mike), One Year into the GDPR, Can We Declare it a Total Failure Yet? Blog, May 24, 2019, https://www.techdirt.com/articles/20190521/17425842255/one-year-into-gdpr-can-we-declare-it-total-failure-yet.shtml visitation date 31/8/2020

26- Middleton-Leal (Matt**), Top 5 Human Errors that Impact Data Security**, published in Cyber Chief Magazine, Edition 5, March 2019, found at https://www.netwrix.com/cyberchief_magazine.html visitation date 17/12/2020

27- Optin Contracts, **Loopholes in GDPR**, no publication date, found at https://www.optincontacts.com/blog/loopholes-in-gdpr/ visitation date 31/8/2020

28-Patrikios (Antonis), **Resolution of Cross-Border E-business Disputes by Arbitration Tribunals on the Basis of Transnational Substantive Rules of Law and E-Business Usages: The Emergence of the Lex informatica**, 21st Bileta Conference, Malta, April 2006, found at https://www.bileta.org.uk/wp-content/uploads/The-Emergence-of-the-Lex-Informatica.pdf visitation date 30/4/2021

29- Popovic (Marko), **Standard Contractual clauses challenged by the GDPR and Scrutinized by CJEU**, published February 9, 2018, found at https://www.lexology.com/library/detail.aspx?g=d4a4a515-4868-4445-8b1c-0d358feab8fe visitation date 6/4/2020

30- Peterson (Luke E.), **Permanent Court of Arbitration Website Goes Offline, With Cyber-Security Firm Contending That Security Flaw Was Exploited in Concert With China-Philippines Arbitration**, July 23, 2015, found at https://www.iareporter.com/articles/permanent-court-of-arbitration-goes-offline-with-cyber-security-firm-contending-that-security-flaw-was-exploited-in-lead-up-to-china-philippines-arbitration/ visitation date 6/1/2021

31- Reciprocity, **What is Cybersecurity?** Published September 11, 2019, https://reciprocitylabs.com/resources/what-is-cybersecurity/ visitation date 17/12/2020

32- Reventlow (Nani J.), **Symposium on the GDPR and International Law: Can the GDPR and Freedom of Expression Coexist**, Published in Ajil Unbound, Volume 114, pp. 31- 34, , found at https://www.researchgate.net/publication/338407067_Can_the_GDPR_and_Freedom_of_Expression_Coexist#fullTextFileContent visitation date 29/8/2020

33- Scott (Mark), Cerulus (Laurens), Kayali (Laura), **Six months in, Europe's privacy revolution favors Google, Facebook,** published in Politico, November 23, 2018, found at https://www.politico.eu/article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/ visitation date 25/8/2020

34- Schrems (Maximillian), **Complaint Against Facebook Ireland LTD- 23 "PRISM" to the Data Protection Commissioner**, Vienna, June 25, 2013, 4 found at http://www.europe-v-facebook.org/prism/facebook.pdf visitation date 15/6/2020

35- Simon (Michael), **Marriott Starwood hotel data breach FAQ: What 500 million hacked guests need to know, published in PCWorld**, November 30, 2018, found at https://www.pcworld.com/article/3324609/marriott-starwood-hotel-data-breach-faq.html visitation date 29/12/2020

36- Zahariev (Martin), (Dimitrov, Petrov & Co.), **GDPR Issues in Commercial Arbitration and How to Mitigate Them**, published in Kluwer Arbitration Blog, September 7, 2019, found at http://arbitrationblog.kluwerarbitration.com/2019/09/07/gdpr-issues-in-commercial-arbitration-and-how-to-mitigate-them/ visitation date 12/12/2020

37- Zhang (Ellen), **What is Operational Security? The Five-Step Process, Best Practices, and More**, Data Guardian's Digital Data Blog, December 1, 2020, found at https://digitalguardian.com/blog/what-operational-security-five-step-process-best-practices-and-more visitation date 17/12/2020

e) Online Encyclopedia

1- Britannica Encyclopedia: https://www.britannica.com/

2- Stanford University Encyclopedia of Philosophy: https://plato.stanford.edu/

f) Official Websites

1- Official Website of the European Union: https://europa.eu/european-union/index_en and https://eur-lex.europa.eu/homepage.html

2- Official Website of the Federal Trade Commission: https://www.ftc.gov/

3- Official Website of Organization for Economic and Commercial Development: https://www.oecd.org/

4- Official Website of AAA/ABA: https://www.adr.org/Arbitration

5- Official Website of ICSID: https://icsid.worldbank.org/

6- Official Website of the European Organization for Nuclear Research (CERN): https://home.cern/

7- Official Website of the Court of Justice of the European Union: https://curia.europa.eu/jcms/jcms/j_6/en/

8- Official Website of the Counseil D'Etat: https://www.conseil-etat.fr/

9- Official Website of the French Data Protection Authority (CNIL): https://www.cnil.fr/en/home

10- Official Website of the International Chamber of Commerce (ICC): https://iccwbo.org/

11- Official Website of the United Nations Commission on International Trade Law (UNCITRAL): https://uncitral.un.org/

12- Official Website of the International Commercial Arbitration Court (ICAC): https://www.worldarbitration.center/

g) Other Websites

1- Used for arbitration and other cases: https://www.italaw.com/

2- https://neuralink.com/

3- https://acqnotes.com/

4- https://economics.creditlibanais.com/

5- https://www.kaspersky.com/

Table of Contents