THE RIGHT TO PRIVACY IN ALBANIA.
ITS COMPLIANCE WITH EU GDPR AND CURRENT CHALLENGES.

MASTER'S THESIS

EGLA LECI

EPOKA UNIVERSITY

FACULTY OF LAW AND SOCIAL SCIENCES

DEPARTMENT OF LAW

Salerno, Italy

July, 2023

THE RIGHT TO PRIVACY IN ALBANIA. ITS COMPLIANCE WITH EU GDPR AND CURRENT CHALLENGES.

EGLA LECI

Thesis Submitted in Fulfillment of Requirement for the Degree of Master of Legal Science

EPOKA UNIVERSITY

2023

APPROVAL PAGE

Student Name & Surname: Egla Leci

Faculty: Faculty of Law and Social Sciences

Department: Department of Law

Thesis Title: The Right to Privacy in Albania. Its Compliance with EU GDPR and Current Challenges.

Date of Defense**:** 18.07.2023

I certify that this final work satisfies all the requirements as a Master Thesis for the degree of Master of Science in Legal Studies

Prof. Niuton Mulleti

Head of Department

This is to certify that I have read this final work and that in my opinion it is fully adequate, in scope and quality, as a Master Thesis for the degree of Master of Science in Legal Studies

Prof. Teresa Russo

Prof. Heliona Miço

Supervisor

Examination Committee Members

Title / Name & Surname	**Affiliation**	**Signature**
1-		
2-		
3-		

The Right to Privacy in Albania. Its Compliance with EU GDPR and Current Challenges.

ABSTRACT

The right to privacy is paramount human rights nowadays. A special attention has been paid by the European Union in the respective field of data protection which with the development of technologies has faced significant challenges. Specifically, Albania is a candidate state in the European Union since 2014. The right to privacy in Republic of Albania is enshrined in the Article 35 of the Constitution of the Republic of Albania, while the law governing the data protection is the Law no. 9887 "On the Data Protection". However, in Albania a series of leaks that resulted in serious breaches of data protection happened from 2021 - 2022, events that further fueled suspicion regarding the cause of these occurrences. Is it the weak legal framework or is it the weak implementation of laws?

Consequently, the thesis aims to answer these questions by studying the development of the right to privacy in Albania during the transition to a pluralistic democratic country and its implementation in the Albanian legal framework. Since European Union is a structure that has dealt with data protection challenges and Albania has an obligation to harmonize its laws in accordance to EU "*acquis communautaire*" an analysis of the Albanian legislation is conducted in comparison to the European Union GDPR.

The study displays a strong legal framework in Albania regarding the protection of the right to privacy and quite a satisfactory level of harmonization. However, the differences diminished the Albanian's level of protection in a digitalized era, a gap that will positively be solved with the implementation of the New Draft Law that Albania will adopt. Regarding the breaches in Albania, issues are concluded regarding the implementation of laws and the lack of professionals in the fields of security and preventive mechanisms provided by law. In this case the comparative studies with the European Union situation have underlined ongoing issues even in the European Union therefore the breaches and cyber-crimes in Albania are not a direct result of weak laws or weak implementation but they adhere as a global challenge of this technologized century.

ACKNOWLEDGEMENTS

There are many people who helped to make my years at the graduate school most valuable.

First, I thank prof. Teresa Russo and prof. Heliona Miço, my major professors and dissertation supervisors. Having the opportunity to work with them was intellectually rewarding and fulfilling. I also thank prof. Stefano Busillo who contributed to the development of this research starting from the early stages of my dissertation work. I thank prof. Niuton Mulleti and prof. Eralda Çani for providing me with additional information on the thesis as well. I thank all the professors that have contributed to my overall legal knowledge through my whole study program where I distinct prof. Gelanda Shkurtaj as the professor to whom I was assigned as a teaching assistant.

The last words of thanks go to my family. I thank my parents Paulin & Brixhilda Leci and my little brother Eden for their encouragement.

DECLARATION

I hereby declare that this Master's Thesis titled "The Right to Privacy in Albania. Its Compliance with EU GDPR and Current Challenges" is based on my original work except quotations and citations which have been duly acknowledged. I also declare that this thesis has not been previously or concurrently submitted for the award of any degree, at "Epoka University", any other university or institution.

(Signature)

Egla Leci

Date: 18.07.2023

Table of Contents

LIST OF ABBREVIATIONS

European Union – EU

European Court of Justice – ECJ

International Convention on Civil and Political Rights – ICCPR

European Convention on Human Rights – ECHR

European Court of Human Rights – ECtHR

United Nations General Assembly – UN General Assembly

General Data Protection Regulation – GDPR

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data – Convention No.108

Charter of Fundamental Human Rights – CFR

The Treaty on the Functioning of European Union – TFEU

The Treaty on the European Union – TEU

Data Protection Authorities – DPA

European Economic Area – EEA

National Security Agency – NSA

Court of Justice of European Union – CJEU

Law. 9887/ 2008 (amended) "On the Data Protection and the Right to Information" – LPDP

The Commissioner for Data Protection and the Right to Information - CPDP

Stabilization Association Agreement – SAA

Data Protection Impact Assessment – DPIA

Data Protection Officer – DPO

Authority of the Electronic and Postal Communications – AKEP (Albanian Abbreviation)

General Directorate of Road and Transport – DPSHTRR (Albanian Abbreviation)

System of Management of the Security of Information – SMSI

Non-governmental organization - NGO

CURRICULUM VITAE

Egla Leci is a dedicated and ambitious individual with a strong educational background and diverse experience in the legal field. Currently pursuing an integrated Law Diploma at Epoka University, she is expected to graduate in August 2023, after having completed her dissertation thesis at the University of Salerno in Italy, a novelty conducted in terms of Erasmus exchange program. Egla has achieved excellent academic performance, maintaining an average of 3.97/4.00. Her experiences include mainly internships and traineeship experiences. We can mention her participation in The Philip C. Jessup International Law Moot Court Competition 2021", the Traineeship "Improving Public Legal Education in Albania" by "OSCE, Albania" and the Traineeship for "Strengthening of the actors that work in the judicial system dealing with refugees and asylum seekers in the Republic of Albania" by "Caritas Albania; Caritas Austria and the Directorate of Free Legal Assistance". She has taken part on summer and autumn schools, such as 7th CLEER Summer School on "EU External Relations Law" by "Maastricht University" and Autumn School on "Illicit Financial Flows" by GIZ & Norwegian Ministry of Foreign Affairs. She has taken part in a significant project such as "Tirana Digital Rights Festival" by "SciDev Center Albania where she had an active role on promoting the digital rights awareness. Regarding her practices and work experiences she concluded an internship in a legal office of Avv. Atli Hoti where she assisted mainly in drafting claims. She concluded another practice at the "Directorate of Free Legal Assistance" where assisted in helping citizens receive free primal judicial assistance. Furthermore she served as a Teaching Assistant at Epoka University, providing support in subjects such as Commercial Law, Civil Law, and Roman law. Lastly Egla concluded a 3 months internship at Helsinki Committee Albania. She is proficient in Albanian and English, with a beginner level in French, and has a good command of MS Office too.

INTRODUCTION

As a fundamental human right recognized and safeguarded by numerous international agreements[1] and legal systems, the right to privacy has been interpreted in international, national and European Union level from more general clauses relating to human rights and individual dignity to broad interpretation of international courts such as European Court of Human Rights (ECtHR) and the European Court of Justice (ECJ). Overall, the protection provided by the right to privacy under international law is crucial for safeguarding people's dignity, autonomy, and control over their personal information in both analog and digital situations.[2] The digitalized era has expanded the dissemination of various information and data, posing a problem to the right to privacy and more precisely the right to privacy under a digital profile, constituting breaches of data protection laws. Consequently, data protection is the process of securing personal information and making sure that people's privacy rights are upheld when their data is gathered, processed, stored, and shared by businesses or other entities. It entails putting procedures in place to protect personal information from being accessed, used, disclosed, altered, or destroyed without authorization. Personal data in this context is any information regarding a person that might identify him/her among the others and the applications of restrictions that are defined by the right to privacy. [3]

The aforementioned changes imposed on by the digitalized era pose different challenges based on different national laws and their respective implementation. However, this study focuses on the Albanian legal challenges on the field of the right to privacy in the context of data protection in a digital processing era as a result of actual changes it has faced; preceding a series of leaks that resulted in serious breaches of data protection taking place in the period of

1 The Universal Declaration of Human Rights (UDHR) recognizes the right to privacy in Article 12 "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks"*; the European Convention of Human Rights (ECHR) recognizes the right to privacy in Article 8 *"Everyone has the right to respect for his private and family life, his home and his correspondence"* the International Covenant on Civil and Political Rights (ICCPR) recognizes the right to privacy in Article *17 "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence"*; the Charter of Fundamental Rights of the European Union (CFR) recognizes the right to privacy in Article 7 *"Everyone has the right to respect for his or her private and family life, home and communications"*.

2 Diggelmann, O., Cleis, M. N. (2014). How the right to privacy became a human right. *Human Rights Law Review, 14*(3), 441-458.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council, (27 April 2016), General Data Protection Regulation (GDPR), Official Journal of the European Union, L 119/1.

2021 -2022. These repeated events fueled suspicion regarding the cause of the occurrences. Is it the weak legal framework or is it the weak implementation of laws?

On the other hand, Albania is candidate state to the European Union since 2014 and has an obligation to harmonize its laws in accordance to EU "*acquis communautaire*". Thus, it is fruitful to analyze the data protection laws of Albania to the data protections laws of European Union. Since European Union is a structure that has dealt with data protection challenges, a parallelization of evolution of the right to privacy in the digital context is displayed in the European context as well. This in order to assess how has European Union as a structure reacted to recent challenges regarding data protection, in respect to legal framework and so, if Albanian law is in harmonization with EU *acquis* on the data protection where is the actual problem of all the occurred breaches? As such this study aims to contribute to assess the level of harmonization of data protection laws in Albania with EU laws and shed light over the actual reasons of the grave data breaches occurrences in Albania, aiming to find the main contributing factors. In order to answer this question the thesis is constructed from a broad level of analysis in European context to reach the heart of the discussion in the analysis of the compliance of data protection laws with GDPR and its evolution.

The thesis is divided into three main chapters. The first Chapter presents the right to privacy and data protection in European Union. It displays firstly the right to privacy in European Context and its main legal frameworks before the General Data Protection, mainly the Directive 95/46/EC. Afterwards, it analyses the reasons that brought General Data Protection Regulation into force and some challenges that were emerging in the data protection field as a result of technological developments. After this legal – historic context, the thesis displays brief analyses on the novelties that GDPR presented to better enhance the legal framework adapting to technological developments. The thesis continues with Chapter two which analyzes the right to privacy and legal framework in Albania regarding the protection of the right to privacy in a constitutional framework and eventually the Law No. 9887 of the Data Protection. This Chapter ends with the comparative analysis between the aforementioned General Data Protection Regulation and Law No. 9887 of the Data Protection. In this part of the thesis we have assessed the level of harmonization of legal framework altogether with the harmonization of Albanian law with GDPR in order to assess whether the Albanian laws have

major differences with GDPR and if so are these differences significant as to lead to a potential situation of data breaches?

Chapter three displays the content of serious data breaches in Albania, describing and carefully analyzing 3 main leaks and issues of e-government and cyber security. In this chapter the dots are completed in concluding the problem of these leaks which stand as more of an implementation problem rather than a huge legal framework gap. The thesis ends with the conclusions in which the future of Albanian data protection laws and its harmonization with GDPR is vaguely anticipated as well.

CHAPTER I: RIGHT TO PRIVACY AND DATA PROTECTION IN EUROPEAN CONTEXT

1.1 A brief overview on the protection of digital privacy on international and European scene.

The protection of *digital* privacy stems from a multitude of legal acts from different international organizations, typically through the proclamation of the bill of rights. The implementation of these acts, therefore, allows the protection of digital privacy at international, regional and domestic level, at the moment of reception and adaptation of these instruments.

At global level, one must emphasize above all the efforts made by the United Nations[4]. Thanks to the non-stop codifying and development of international law by the UN General Assembly[5] – and its subsidiary body, the International Law Commission – the United Nation succeeded in the creation of a comprehensive body of human rights law, in other words a universal and internationally protected code.

Particularly an *indirect* affirmation of the right to digital privacy is found in the Universal Declaration of Human Rights (UDHR), which was approved by the United Nations General Assembly in 1948[6]. Article 12 of the UDHR states that: "*No one shall be subject to arbitrary interference with his privacy, family, home or correspondence*". According to one interpretation, this clause includes the right to privacy.[7]

Preceding the right to privacy it is important to highlight the International Convention on Civil and Political Rights (ICCPR)[8] is an international human rights treaty of the United Nations

[4] The United Nations came into existence on October 24, 1945, after 29 nations had ratified the Charter. Indeed, after the conclusion of the World War II, representatives of 50 nations met in San Francisco April-June 1945 to complete the Charter of the United Nations.
[5]Under Article 13 of the UN Charter.
[6] UDHR is a legal document that contains civil, political, economic, social, and cultural rights. UDHR lays out guidelines and criteria for defending and advancing human rights while highlighting the equality and intrinsic worth of every person. Although the UDHR is not a legally binding instrument, it has shaped subsequent human rights agreements and serves as the cornerstone of international human rights legislation. It has played a significant role in influencing national constitutions, laws, and policies all over the world, acting as a benchmark for promoting and defending human rights all over the world.
[7] United Nations General Assembly. (1948) "Universal Declaration of Human Rights" 217 (III)A.
[8] A legally enforceable international agreement known as the International Covenant on Civil and Political Rights (ICCPR) was adopted by the United Nations General Assembly on December 16, 1966. The Universal

which entered into force in 1976. It envisages among others the right to be free from arbitrary or unlawful intrusion into the private lives of individuals, including their privacy, family, home, and correspondence as stated according to Article 17 of ICCPR. This covers defense against unlawful monitoring, wiretapping, searches, and other types of interference that infringe on a person's right to privacy. The text also highlights the need for legal defense against any interference with or assaults on a person's reputation or honor. This means that anyone who has their privacy rights violated has the right to file a lawsuit to seek compensation. [9]

The European Convention on Human Rights (ECHR)[10] explicitly protects the right to privacy under Article 8. The provision guarantees that everyone is entitled to the fundamental human right to respect for their family, home and correspondence, which includes as well the right to the protection of their personal data. As such the right to privacy is an umbrella right that expands upon more detailed endeavors and different legal branches, however in this paper is analyzed under the concept of Data Protection. The right to respect for one's home, correspondence, private and family life is covered by Article 8. [11] It is concluded by the ECHR that even though a particular right is not stated in Article 8, the Court defines the Article's scope broadly. In the case law (Denisov v. Ukraine [GC], 96)[12], the Court concluded that the idea of private life is not restricted to an "inner circle" where a person is free to live his or her private life and keep the outside world out. The case (Bărbulescu v. Romania [GC], 2017, 71; [13] Botta v. Italy, 1998, 32[14]) emphasizes that the right to a "private social life" includes the freedom for each person to approach others in order to form and grow ties with them as well

---

Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) together make up the International Bill of Human Rights. The ICCPR recognizes the inherent dignity and equal rights of every person and works to safeguard and advance those rights.

[9] United Nations General Assembly. (1966) International Covenant on Civil and Political Rights, Treaty Series, vol. 999, p. 171.

[10] The Council of Europe established the European Convention on Human Rights (ECHR), which was ratified in Rome on November 4, 1950. The Council of Europe member nations are the target audience for the ECHR, which works to defend and advance human rights. It is one of the most important human rights laws in Europe and has significantly improved the defense of basic freedoms and rights.

[11] Council of Europe, (1950), European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13, and 16.

[12] European Court of Human Rights, Case of Denisov v. Ukraine (25 September 2018), Strasbourg Application no. 76639/11.

[13] European Court of Human Rights, Case of Bărbulescu v. Romania (5 September 2017), Strasbourg, (Application no. 61496/08).

[14] European Court of Human Rights, Case of Botta v. Italy (24 February 1998), Strasbourg, (153/1996/772/973).

as with the outside world. The case (Axel Springer AG v. Germany [GC], 2012, § 83[15]) lays down the idea that the term "private life" is a broad term and cannot be narrowed in one definition. It refers to a person's physical and psychological well-being and can therefore include many facets of their identity, including their name, sexual orientation, gender identity, and elements pertaining to their image. As such it goes to that extent that addresses the idea that people shouldn't have their personal information public without their permission, which encompasses the digital privacy the thesis is about. [16]

Another important instrument to mention is actually the first legally binding international agreement, The Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data or known as the Convention No. 108.[17] This Convention holds the position as the first instrument that strives to both control the cross-border movement of personal data while also safeguarding persons from the abuses that may result from the collecting and use of personal data. Convention No. 108 establishes that everyone has the right to knowledge, access, and rectification of their personal data processed by third parties as well as the right to have personal data that has been unlawfully processed erased. Automatic Processing of Personal Data[18] in the Article 5 requires that personal data be processed fairly, securely, and only for purposes that are specified and justified.

In accordance to the technological developments, cyber – crime became an important international crime and as such The Convention on Cyber Crime or the so called "Budapest Convention"[19] is another international treaty addressing both the substantive criminal law and

[15] European Court of Human Rights, Case of Axel Springer AG v. Germany (7 February, 2012), Strasbourg, (Application no. 39954/08).
[16] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights, 31 August 2022.
[17] An international agreement known as Convention No. 108, or the Convention for the Protection of Individuals with respect to the Automatic Processing of Personal Data, is dedicated to preserving peoples' rights and liberties with regard to the processing of their personal data. It was the first worldwide data protection law and was enacted by the Council of Europe on January 28, 1981. Establishing a framework for the protection of people's privacy and personal data in the context of automatic processing is the main goal of Convention No. 108. It is applicable to both the public and private sectors and attempts to guarantee that the gathering, storing, using, and disclosing of personal data is done in a way that respects people's rights.
[18] Council of Europe, (1981) European Treaty Series - No. 108,Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
[19] The Budapest Convention, commonly known as the Convention on Cybercrime, is an international agreement designed to combat cybercrime and foster collaboration among nations in resolving cyber-related crimes. On November 23, 2001, the Council of Europe in Budapest, Hungary, approved it. Cybercrimes should be made illegal, international collaboration should be encouraged, and human rights should be protected. It addresses a

the procedural law aspects of cybercrime. It defines a number of cybercrime offenses, including unauthorized access, unauthorized interception, tampering with data or systems, and computer-related fraud. The convention also addresses copyright violations (Article 10 of the Convention on Cybercrime, 2001), and child pornography (Article 9 of the Convention on Cybercrime, 2001).

Despite the Council of Europe's legal instruments, another structure effectively enriches the protection of human rights and privacy, this time at a regional level. This structure is European Union.[20] Since its creation its values of creating a single market and protecting human rights transformed, further shaped by the changes throughout the years. Through collaboration of European Union's institutions, the European Union created a well –known body of laws applicable to all EU Member States, such as Charter of Fundamental Rights, The European Union Directive 1995, 95/46 EC and General Data Protection Regulation at last.

More specifically, the fundamental liberties and rights of people living in the European Union are outlined in the Charter of Fundamental Rights of the European Union (CFR)[21]. The CFR contains rules that are pertinent to the preservation of privacy. The right to respect for one's home, communications, private and family life is guaranteed by Article 8 of the Charter. Everyone has the right to have their personal information secured, and it must be handled fairly for given reasons with the consent of the subject. Additionally, it forbids willful invading of a person's privacy.

The European Union (EU) is based on the fundamental principles of the European Convention on Human Rights that protects the human rights of people in countries that belong to the

---

variety of cybercrimes, such as copyright infringement, fraud, child pornography, computer hacking, and online terrorism.

[20] A political and economic union of 27 member nations, most of which are in Europe, makes up the European Union (EU). Supranationalism, integration, and cooperation among its member states serve as its guiding principles. With the use of integrated institutions, a single market, and shared policies, the EU seeks to advance peace, stability, and prosperity. It started as a structure in 1950 with Coal and Steel Community, continuing with several integration phases enclosed by treaties and acts such as; European Economic Community (EEC), Single European Act (SEA), Treaty of Maastricht; Treaty of Amsterdam, Treaty of Nice and eventually in the Treaty of Lisbon.

[21] The fundamental liberties and rights that every person in the European Union (EU) is entitled to are outlined in the Charter of Fundamental Rights of the European Union (CFR), which is a binding legislative document. On December 1, 2009 CFR became legally binding with the establishment of Treaty of Lisbon. The EU's defense of fundamental rights is strengthened and consolidated by the CFR. CFR acts as a benchmark for EU law and policies, covering civil, political, economic, social, and cultural rights as well. Therefore, when implementing EU law, member states and EU organizations and agencies are subject to the charter.

Council of Europe but plays a major role in the protection of the rights of EU citizens as well. Therefore this convention's principles stand as the main pillars of European Union as a structure altogether with those expressed in the Charter of Fundamental Rights. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) and Article 17 of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. Therefore, preceding the right to privacy, expressed in Article 8 of European Convention of Human Rights and the obligation of the institutions that functions upon treaties and fundamental human rights, European Union adopted the European Union Directive 1995, 95/46 EC[22].

The European Union Directive 1995, 95/46 EC also known as Directive 95/46/EC of the European Union, was a significant legal framework that attempted to safeguard people's privacy and fundamental rights with relation to the processing of their personal data. It created a thorough framework for data protection throughout the European Union (EU) and was adopted on October 24, 1995. This Directive is composed of the main principles of data protection such as transparency, legitimate purpose and proportionality. [23] It aimed harmonizing the laws between the European Union's Member States in order to ensure the basis of common protection of personal data that was now in convergence with the free market and data transfer as a tool of vitalizing European Union's trading entities to compete and develop their business.[24] As such, the directive included a number of core ideas and specifications for data protection, including the notion of data subjects as individuals recognized by the directive (Article 26 of the Directive 95/46/EC), data controllers and processors (Article 2 (d) (e) of the Directive 95/46/EC), legitimate grounds for data processing (Article 28 of the Directive 95/46/EC), and cross-border data flows (Chapter 4 of the Directive 95/46/EC). Some illustrative cases of CJEU regarding the scope of this directive are displayed in *Rechnungshof case*[25] and *Lindquist case*[26]. *The Rechnungshof* case displays that the

[22] Directive 1995/ 46 EC. Directive (EC) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[23] EUR-Lex. (2014). Summaries of EU Legislation "Protection of Personal Data".
[24] Schwartz, P. M. (1994), European data protection law and restrictions on international data flows, *L. Rev., 80,* 481.
[25] European Court of Justice, Rechnungshof vs. Osterreichischer Rundfunk, C-465/00, C138-/01, and C-139/01 [2003], ECLI:EU:C:2003:294.

boundaries of the Directive's range of application could become ambiguous and unknown under a different interpretation. Processing of personal data is subject to a number of restrictions and criteria under the system of checks and balances. This case shows the importance that this Directive has in the realm of the right to privacy, having no limited scope in this regard. Meanwhile *Lindquist case* is of high value for it confirmed that actual loading of personal data on a web page constitutes processing by automatic means. [27] The directive furthermore established Data Protection Authorities (DPAs) (Chapter 6 of the Directive 95/46/EC), which are independent public organizations tasked with enforcing and monitoring compliance with data protection legislation, in each EU member state.

In truth, among the legal acts of the European Union, the General Data Protection Regulation (GDPR) stands out as the beacon of digital privacy protection in the region. The Regulation was adopted in 2016 and came into effect in May 2018 following a two-year transition period. GDPR it is the main legal act of the European Union that regulates the processing of individuals' personal information within the European Union and the European Economic Area (EEA)[28] , as well as that controls the transfer of personal information outside of the EU/EEA.

1.2 The reasons that brought the EU General Data Protection Regulation (GDPR) into force.

The dynamics of inter trade amongst European Union's Member States and the use of data in economy brought extensive changes to the regulatory environment that demanded for a new legal basis in order to manage and facilitate the conduct of different trade companies operating within the European Union or out of the territory of European Union without breaching the

---

[26]European Court of Justice, Bodil Lindqvist v Åklagarkammaren i Jönköping, C-101/01 – [2003], ECLI:EU:C:2003:596.

[27] Data Protection Officer, European Anti – Fraud Office (2016), Summaries Of EU Court Decisions Relating To Data Protection 2000-2015 , Pg. 50

[28] The European Economic Area (EEA) is a cooperative economic arrangement involving all the EU member states as well as Norway, Iceland, and Liechtenstein. It enables these nations to take part in the free movement of people, capital, products, and services that makes up the EU Single Market.

right to data protection and undergoing illegal processing of the personal data of European Union citizens.[29]

This particular attention on the GDPR materialized after some grave data violations such as the Snowden case when Edward Snowden, a whistleblower who provided information about the NSA's PRISM program for widespread surveillance, a program he worked for as a system administrator. [30] National Security Agency (NSA) is a highly classified US intelligence organization in charge of gathering, processing, and analyzing data and foreign information on cyber security. It is one of the biggest and most enigmatic intelligence agencies under the Department of Defense in US.[31] As such Prism program was a surveillance program aimed to gather data doubted to be a threat of national security of US but later was leaked that NSA has actual direct access to big technological companies such as Facebook and Google. [32]

Further information concerning the NSA's and other affiliated intelligence services' surveillance techniques came to light in the months after his revelations. It was discovered that the NSA had uncontrolled access to EU individuals' personal information that was kept on US servers. [33] Consequently, this case raised awareness of the so called "transfer of data" which in the given case occurred between US and EU.

In order to regulate the transfer of this data an agreement was signed between EU and US in order to safeguard the transfer of data for commercial purposes. This agreement was the Safe Harbor Agreement and it had 7 (seven) main principles under which it functioned. The first one is the concept of "notice where the data subject should be made aware of the collection of their data, how it will be used, and how to get in touch with the data holder with any questions. Furthermore the data subject should have the option to refuse processing as well as to transfer pertinent information to another third party, this principle entailing the element of "choice". Regarding the transfer of data it is mentioned the principle of the "onward transfer" which

[29] European Commission, Brussels, (19 February 2020), Communication from The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European Strategy For Data".
[30] Greenwald, G., Poitras, L. and MacAskill, E. (2013) Edward Snowden: the whistleblower behind the NSA surveillance revelations, The Guardian.

[31]National Security Agency, (2023) Official Website https://www.nsa.gov/about/.
[32] Gellman, Barton; Poitras, Laura (June 6, 2013). "US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program". The Washington Post.
[33] Ibid 30.

emphasizes that data transfer can only take place with a third party who complies with the necessary data protection principles. Hence, security proceeds as one of the principles where reasonable efforts must be made to protect the data against theft and loss. However this data should be reliable in order to be considered to have "integrity". In order to assess the data's integrity principle and check the necessary information, access should be available to data subjects for review, correction, and deletion. As such the last principle entails the "enforcement". This principle encompasses the fact that there must be efficient ways to put these policies into action. [34]

As evaluated, these principles imply the transparency and fairness of the processing of personal information. However, according to Jacob Kohnstmann, the head of the Article 29 Working Party there was a "high chance" that the Safe Harbor principles had been broken.[35] According to the European Union's Data Protection Directive, the transfer of personal data to a third country is only, in theory, permitted if that country guarantees an acceptable degree of data protection.[36]

In this case it is implied that the Safe Harbor Agreement was not actually preventing breaches as proven by the aforementioned case of US data collection and processing. As a result of this "failure" the Safe Harbor Agreement was declared "invalidated" by the Court of Justice of the European Union (ECJ), in *Schrems I case* [37] for not providing adequate level of protection. [38] The "Safe Harbor" system, which permitted the movement of personal data from the European Union to American businesses who self-certified their compliance with specific data protection requirements, was the subject of the dispute, which centered on its legality. The CJEU essentially concluded that Safe Harbor had fallen short of EU data protection requirements. [39] The CJEU ruled that while third-country data protection laws need not be identical to those in the EU, they must still offer a similar level of security to that mandated by

[34] Weiss, Archick, (2016). U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research In Brief. 7-5700.

[35] European Commission. (2015). Communication From The Commission To The European Parliament And The Council on The Transfer Of Personal Data From The EU To The United States Of America Under Directive 95/46/EC Following The Judgment By The Court Of Justice In Case C-362/14 (Schrems).

[36] Ibid 22.

[37] European Court of Justice, Ruling C-362/14, *Schrems I*, 6th October 2015 ECLI:EU:C:2015:650, parg.57.

[38] Ibid 37.

[39] Ibid 34.

the (then) EC Data Protection Directive. By doing this, the CJEU increases the fundamental rights' substantive content.[40] Another important principle highlighted in *Schrems I* [41] was the surveillance and national security. The court highlighted concerns on the potential interference with people's right to privacy and data protection by foreign public authorities, particularly those engaged in surveillance and national security activities. It was emphasized that such interference should be subject to unambiguous protections and limitations.[42]

It is implied that this is the main case that contributed in the idea to invent a new version of data protection that would have the form of a regulation. All these demonstrative cases and the decision of the court display the necessity of "unifying" data protection laws in order to protect European citizens' data in an increased efficient manner. Other researchers approve that one major reason for the reform was the disparity in implementation and application among Member States, which resulted in disparities in data protection standards.[43]

After many years of planning, an agreement was made on the General Data Protection Regulation (GDPR), one of the most significant pieces of legislation to be passed in the previous 20 years.[44] In this sense it should be said that based on the distinction that directives as legal instruments have more of a harmonization role rather than unification[45] implementation of a regulation shows the added attention of the European Union to design a rigid regulation, raising data protection concern on a supranational level rather than intergovernmental level.

1.3 Contents and Scope of the GDPR

---

[40] Global Freedom of Expression. (2021). "Schrems V. Data Protection Commissioner, Columbia University.

[41] A*ccording to the EC Data Protection Directive (RL 95/46/EC), data transfers to third countries, i.e. countries outside the European Economic Area (EEA), were permitted only if there is an adequate level of protection in the country in which the recipient is located. So far, the Commission's decisions attesting the adequacy of the level of protection in individual countries were based on the Directive. As no classical data protection laws existed in the U.S., the U.S. committed itself to the Safe Harbor Framework. The latter, stipulated privacy principles to which American companies may self-certify themselves. With respect to such self-certified Safe Harbor-companies, the Commission's decision in the year 2000, which was then overturned by the CJEU, recognized the U.S. as a safe third country. Until Schrems, it was therefore possible to transfer data to such companies*.

[42] Ibid 37. Pg.8.

[43]Hustinx, 2013, as cited in Vogelsang, H. (2019). *An analysis of the EU data protection policy and the significance of the Maximillian Schrems case.*

[44] European Data Protection Supervisor. (2023). The History of General Data Protection Regulation.

[45] European Parliament. (2017). The EU as a community of law Overview of the role of law in the Union, Briefing, Think Tank.

The GDPR was adopted in 2016 and went into effect in May 2018, following a two-year transition period. [46] It has 11 chapters and 99 Articles. Its adoption brought in light the gravity of data protection as well. Recital 1 of the GDPR declares that the protection of natural persons in relation to the processing of personal data is a fundamental right. Recital 2 of GDPR states that the principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. [47] Recital 2 emphasizes that this regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.[48] As a result, organizations are required by the terms of the GDPR not only to ensure that personal data is collected lawfully and under strict security conditions, but also to secure that everyone involved in the collection, processing, or storage of the data takes reasonable steps to prevent its unauthorized use and exploitation.[49]

The main principles or GDPR were well defined and stay as the main pillars of all the conduct. [50]It should be said that they are equivalently equal to the principles laid down in the European Union Directive 95/46 EC. These principles are set out in Article 5 of the GDPR are lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality (security) and accountability.[51] Consequently lawfulness, fairness and transparency are the main concepts that allow the lawful processing of data. Lawfulness stands for processing of the data by a controller in compliance with the rules provided by the Regulation such as; having consent of the data subject, having a legitimate purpose of requiring the data specified in Article 6 - (1) f GDPR.[52] Fairness stands for the fiduciary relation between the controller and data subject in order for the controller to fairly process only that part of the data that is needed for its purpose and not further or even exercise

[46] Article 99 GDPR.
[47] Recital 2 of the General Data Protection Regulation.
[48] Recital 2 of the General Data Protection Regulation.
[49] Riza, G. (2021).“GDPR and personal data protection in non- EU countries: Albanian case of data protection legislation”, CEUR Workshop Proceedings.
[50] International Commissioner’s Office (2023), A guide to the data Protection.
[51] Article 5 of the GDPR.
[52] Article 6 -(1)- f GDPR.

the duty to destroy the data after the exact date of the termination of the moment for which the data needed to be stored and processed. [53]Transparency stands for the controller to give information prior than collecting the data, expressed in (Arts. 13-(2), 14-(2), 34-(1) GDPR), where it is emphasized among others the information of how they process the data.[54]

Taking into consideration the fact that the principles of GDPR are equal to the Directive 1995, 95/46 EC, it is significant to analyze the novelties that were embedded within GDPR.

First of all the GDPR expanded the definition of what constitutes personal data beyond just name, address, and photographs. According to the European Commission Regulation (2020) now includes even an IP address or other comparable digital data that can be used to identify us on the internet, displayed in the Article 4-(1) GDPR. [55] It coined new terms like profiling and pseudonymisation.[56] The GDPR uses the same definition for special categories of personal data as the Directive, but includes genetic and biometric information. This type of data has a higher level of protection. [57] Another addition to GDPR is the strengthening of the concept of consent. Furthermore it is specified in Art. 7 (3) GDPR that data subject has the right to withdraw their consent at any time.

Regarding the controller Article 7(1) states that the controller must be able to have proof regarding the consent of the subject. This clearly poses a higher responsibility to the controller in making sure that the data subject is aware of the consent that is giving and must be able as such to prove it beyond reasonable doubts. An interesting clause is distinguished in the Article 8 GDPR that acknowledges the right of children to give consent regarding the processing of their data. It provides that generally the minimum age allowed to give consent is sixteen (16)

[53] Wilson, R. (2023). Data Controllers as Data Fiduciaries: Theory; Definitions and Burden of Proof *University of Colorado Law Review, Vol. 95, No. 1, 2023*
[54] Articles 13 (2), 14 (2), 34 (1) GDPR.
[55] Article 4 (1) GDPR.
[56] Profiling is defined as any form of automated processing of personal data, specifically data relating to work performance, wealth, health, personal interests and movements, that allows for the creation of a profile of the data subject (Article 4 - (4) GDPR). These profiles can be used to analyze or predict the subject's behavior. Pseudomynisation refers to the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. As a result, this required information must be kept separately and protected from unauthorized access.
[57] Vogelsang, H. (2019). An analysis of the EU data protection policy and the significance of the Maximillian Schrems case.pg.31.

but regarding paragraph 1 of the Article, Member States can decrease the age up to thirteen (13) in special cases provided by law. [58]

The right to erasure is one of the rights expressed even in the Directive 95/46/EC, however a novelty is presented in the GDPR with the introduction of "the right to be forgotten" as a separate highlight in the Article 17 and 19 GDPR. The right to be forgotten entails the idea that the controller should erase the information of the data subject as long as it is not used anymore for legitimate purposes or after a specific timeline of the interest. This article acknowledges the right of the data subject to request the erasing of his information when the data subject does not see fit to continue giving the consent anymore. [59] This can be illustrated with a case law of the European Court of Justice, respectively *Google Spain* case when a Spanish citizen sued Google and other entities for displaying garnishment information even though the proceeding was resolved years ago.[60]In Google v. Spain, the European Court of Justice decided that European residents have the right to ask commercial search engines like Google to erase links to its users' private information upon request, so long as the material is no longer relevant.[61] Continuing with supervisor authorities, their functions and relation to the right of remedies are envisages in a detailed manner in the Article 77 of GDPR. This Article stipulates that the actual individuals or data subjects have the right to remedy by directly issuing complaints to a supervisory authority that in this case might be a national institution that holds the competences of a supervisory authority that can issue fines for the controller that might be caught in breaches of data protection regulation. Article 78 (1)[62] envisages the right of the controller to appeal in the court regarding the actual binding decision of the supervisory authority that contributes to the enforcement to the right to judicial remedy. Article 80 (1) envisages that "the data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of

[58] Article 8 (1) of GDPR "Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years."
[59] Article 77 (1) GDPR.
[60] European Court of Justice, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, [2014] 1 C.M.L.R. 677.
[61] Ibid 60, para.81.
[62] "*Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.*"

a Member State, has statutory objectives which are in the public interest".[63] These organizations can file collective claims as per Article 80 (2) of the GDPR as well as the right to compensation.

Regarding the controllers obligations to ensuring correct processing and storage of data Article 5 (2) GDPR highlights that the controller has to proof his compliance with the main principles of preserving the data and prove the compliance with the specific obligations envisaged in GDPR. Article 32 GDPR states that the controller and processor must implement appropriate technical and organizational measures to ensure a level of security commensurate with the risk, including, as necessary, the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident as well as a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing systems and services.[64]

The GDPR includes a new requirement to notify the data subject and the responsible national DPA about data breaches that may jeopardize an individual's privacy envisaged in in Article 33 and 34 GDPR.[65] In any case, the supervisory authority must be notified within 72 hours; otherwise, the delay must be justified reasonably. [66]Article 34 (1) of the GDPR specifies that if the data breach is likely to jeopardize the data subject's privacy rights, the affected data subject must be notified as soon as possible. In exceptional cases, reporting to the DPA is not needed if the data controller can demonstrate that, despite the data breach, there is no risk to the data subject's rights and freedoms.[67]

In general, the Regulation has increased the requirements placed on controllers and processors and reinforced the rights of those who are the subjects of personal data. Regarding individual rights, the Regulation recognizes more of them, improving openness and giving subjects greater control over their data. The rule has increased the obligations placed on controllers,

[63]Article 80 (1) GDPR.
[64]Article 32 (1) GDPR.
[65]Article 33, 34 GDPR.
[66]Article 33 (1) GDPR.
[67]Article 34 (1) GDPR.

among other things by altering the penalty regime, specifying the need to inform the subject of personal data, and defining the appointment of the officer for personal data.[68]

Even though GDPR introduced subsequently improved changes, its interpretation and implementation problems made an appearance soon after it's enter in force. *Schrmes II case*[69] and Case 460/2020 *TU and RE v Google LLC* are some CJEU cases that highlight this issue and show that even though GDPR is seen as the most significant legal framework it still has its own grey zones.[70]

As the thesis displayed above, Schrems, a fierce activist, the main subject of *Schrems I* case, pointed problems of the GDPR implementation and more specifically on the validity of the Standard Contractual Clauses (SCC)[71] for data transfer under GDPR. The *Schrems II*[72] case stressed the significance of safeguarding personal data during cross-border transfers and the demand for meticulous evaluations, additional safeguards, and oversight to guarantee adherence to EU data protection regulations. The Case 460/2020 TU and RE v Google LLC[73] highlights a conflict of fundamental rights between the right to freedom of expression and the right to privacy, specifically right to erasure. [74] The CJEU emphasizes that the right to the protection of personal data must be viewed in light of its purpose in society and does not have absolute validity. It must be weighed against other fundamental rights in accordance with the proportionality principle. Because of this, the GDPR makes it clear that the right to data

[68] Albanian Helsinki Committee. (2022). "Legal and institutional overview for his protection and safety personal data in our country and their compliance with the acquis". pg.24

[69] European Court of Justice, Ruling C-311/18, *Schrems II* on 9 May 2020, ECLI:EU:C:2020:559

[70] Data Privacy Day. (2023). The most impactful ECJ judgments from the past years.

[71] Standard Contractual Clauses (SCCs): SCCs are an additional method frequently employed to simplify the transfer of personal data from the EU to nations outside the EU. The legality of SCCs as a legal foundation for such transfers was the main concern in *Schrems II*.

[72] The CJEU looked at American surveillance techniques, particularly those made public by Edward Snowden, and questioned whether personal data transmitted from the EU was adequately protected. The EU Charter of Fundamental Rights guarantees everyone a fundamental right to privacy and data protection, which was stressed by the court. The CJEU held that transfers of personal data to third countries must guarantee a degree of protection that is essentially similar to that provided within the EU. For effective safeguards for people's privacy and data rights, additional measures must be put in place if the recipient country's laws and practices do not afford sufficient protection. Authorities in charge of overseeing data protection were tasked with determining if protection was adequate and had the authority, if necessary, to halt or forbid transfers.

[73] European Court of Justice, Ruling C-460/20 on 8 December 2022 Re V. Google ECLI:EU:C:2022:962

[74] The issue is whether Google should remove links and so-called "thumbnails" from search results if they point to content that the data subject believes to be inaccurate. Google refused the data subject's request for erasure, citing the freedom of speech and access to information as fundamental rights. The subject of the data emphasized their fundamental right to privacy.

deletion does not apply when processing is required for the enjoyment of other rights, like the right to information freedom.[75]

CHAPTER II: HOW CLOSE OR FAR FROM THE GDPR IS THE ALBANIAN LEGAL FRAMEWORK?

2.1 Constitutional overview of the right to privacy and data protection in Albanian legal framework.

In order to exhaustively show the framework of Albania regarding the data protection, it is fit to start the analysis with a constitutional overview of the right to privacy that envisages largely the right to data protection.

The Constitution of Republic of Albania was officially adopted in 1998, which defined Albania as a parliamentary republic and a unitary state. In the framework of 1976's Constitution it should be mentioned that the right to privacy and protection of personal data was not sanctioned. At that time Albania was still under the communist regime that is characterized by an oppression of fundamental rights such as the right to a private life or the right to speech. Under this timeline Article 49 of the Albanian Constitution of 1976[76], guaranteed the right to a private and family life within a limited communist ideology, emphasizing the responsibility of parents to instill the communist ideal in their children.[77] As such, it did not expressly mention the protection of personal data or the right to privacy until the Constitution of the Republic of Albania of 1998 after the fall of communism. [78]

However, with the adoption of the new Constitutional framework of 2016 the Articles 35, 36, 37 envisage "*the right to the private life*". Since the violation of private life tends to be threatened by the development of technologies, the sanctioning in the Constitution of the right

[75] European Court of Justice, Ruling C-460/20 on 8 December 2022 Re V. Google ECLI:EU:C:2022:962 par.4.
[76] *"Marriage and family are under the protection of the state and society.*
The marriage is solemnized before the competent state bodies.
Parents are responsible for the good upbringing and communist education of the children.
Children have the duty to take care of parents who are incapable and without sufficient means of living. Children born out of wedlock have the same rights and duties as children born in wedlock.
Children left without parents and without support are raised and educated by the state."
[77] H. Miço. (2023). The right to private and family life and the need for protection against the digital environment". European Journal of Economics, Law and Social Sciences Vol. 7 No. 2.
[78] Constitution of the Republic of Albania, adapted by the law no. 8417, dated 21.10.1998, as amended.

to a private life and the rights related to "*the inviolability of housing*" were an essential step. The right to privacy in the Republic of Albania is closely related to "*the right to a normal family life*", even though the latter has been affirmed separately, mostly a right with a rather economic, social and cultural character. [79]

Regarding the right guaranteed from the State, there have been several constraining legal doctrine views on the reason why this right has been directly sanctioned rather late.[80] In the Constitution of the Republic of Albania the right to privacy represents special values which are highly related to some of the fundamental rights. More specifically in the data protection as envisaged in the Article 35 paragraph 1 of the Constitution of the Republic of Albania an individual is not compelled to make his personal data public, unless the law requires it. This first paragraph emphasizes the right of an individual to keep his information private. The second paragraph of Article 35 emphasized that even in cases when the data should be given for lawful purposes it should be given only by the consent of the data bearer.[81] This highlights the principle of lawfulness and fairness of processing of personal data envisages in the Law No. 9887/2008 where Article 5, paragraph 1/a. states: "*Protection of personal data is based on: a) a processing that is honest, fair and lawful*". The second paragraph of Article 35 envisages that everyone has the right to be acquainted with his/her information that is being stored by another entity. The last paragraph of this Article expressed the right to request the elimination of false and incomplete information or request to update the information that an entity is storing according to law in power, explicitly stating "*Everyone has the right to become acquainted with data collected about him, except for the cases provided by law. Everyone has the right to request the correction or deletion of untrue or incomplete data or data collected in violation of law.*"

The concept of privacy occurs in Articles 36 [82] and 37 of the Constitution of the Republic of Albania which protect the right of privacy of the housing from the interventions to have a control, which are not allowed with simply the will of a person or with unauthorized interventions of the police. Article 32 of the Constitution envisages "the right to not be

[79] Omari. L, Anastasi. A. (2017). E drejta kushtetuese, Dajti 2000, Tirane ISBN: 978 99956 01 41 6 pg,136.
[80] Ibid 77, pg,136 -137.
[81] "The collection, use and making public of data about a person is done with his consent, except for the cases provided by law"
[82] "The freedom and secrecy of correspondence or any other means of communication are guaranteed"

incriminated", which is an expressed provision in the Criminal Code of the Republic of Albania as well. This other right emphasizes the right that the individual has to keep the information secret regarding himself and other members of his family.[83]

Albania has furthermore ratified the following international conventions concerning the right to privacy such as; the European Convention on Human Rights in 1996, which contains in Article 8 the right to respect for private and family life, home, and correspondence;[84] International Convention on Civil and Political Rights in 1991, which includes the right to privacy in Article 17 [85]and the Convention for the Protection of persons with Regard to Automatic Processing of Personal Data that was ratified by Albania in 2005.[86] This convention anticipates the condition of giving consent before processing personal data, assessing knowledge regarding the data processing, requiring rectification/erasure of such data and some guaranties regarding the transfer of data abroad. Lastly Albania has ratified the Convention on Cybercrime in 2002 [87] with the goal of preventing and combating cybercrime, particularly the exploitation of personal data.

These Conventions that are part of international law show an extensive legal framework on protection of personal data and respect to the right to privacy. As such Albania is a state that its legal framework is complied with the international legal acts that protect the right to privacy as a fundamental right.

The first time a data protection law was enacted was in 1999, precisely Law No.8517 on the Right to Information and Protection of Personal Data. This Law has only 21 Articles on the data protection, a fact that shows the shallow legal framework in this regard. However, it envisaged the notification of data subjects in the Article 6, the safety of personal date in the Article 9, the consent in the Article 10 and a vague description of transfer of data in the Article 14. This law was in power until the law 9887 was enacted in 2008. Therefore in Albania the

[83] Ibid 77, pg,139.
[84] Official Gazette of the Republic of Albania, (2000) ECHR Ratified by Law, no. 8641, date 13.7.2000.
[85] Ratified on 04 Oct 1991, United Nations Human Rights Treaty Bodies, UN Treaty Database. Albania's accession to the International Covenant on Civil and Political Rights has been approved by law. No. 7510, dated 08.08.1991.
[86] On the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Law of 2004, Pub. L. No. 9288/2004.
[87] Ratified on 20/06/2002 Council of Europe. (2022). Chart of signatures and ratifications of Treaty 185.

specific law that governs the protection of personal data is the Law 9887, date 10.03.2008 (amended) that is abbreviated in the upcoming analysis as LPDP. [88]

2.2 Law 9887/ 2008 on "*The Right to Information and Protection of Personal Data*".

Albania's Law on Personal Data Protection (LPDP) was enacted on March 2008 and went into effect on May 23, 2008. The LPDP is the basic law governing personal data processing in Albania, and it strives to protect individuals' fundamental rights and freedoms in relation to personal data processing.[89] Article 2 of the LPDP emphasizes that the legal processing shall respect fundamental human rights and in particular the right to privacy. This provision indicates the level of recognition that the Albanian law has towards data protection as a right that is correlated to the right to privacy as such as the establishment of this law. Regarding its general scope, the LPDP applies to all personal data processing methods, as well as data controllers and processors based in Albania. Personal data is defined in Article 3 of the LPDP as "any information relating to an identified or identifiable natural person," while processing is defined in Article 3/7 as "*any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination*." The principles of data processing are the same as the one used in General Data Protection Regulation. Article 5 of the LPDP explains the actions that resonate with the principles of GDPR, such as; Lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy and storage limitation. Following the principles, prior consent is one the most important actions envisaged in Albanian law but can be disregarded only by law in specific cases when there is a need for the execution of a legal obligation of the subject of data itself. An example is the obligation of certain official individuals that hold state positions to declare their finances. [90] However a little contradiction was faced before 2004 for the Law no.9049/2003 "On The Declaration And Audit Of Assets, Financial Obligations Of Elected Persons And Certain

[88] On the Protection of Personal Data, Law of 1999, Pub. L. No. 8517/1999.
[89] Law No.9887 date 10.3.2008 "For the Protection of the Personal Data" Amended by Law No.120/2014, F.Z 160).
[90] Law No. 9049, dated 10 April 2003 "On The Declaration And Audit Of Assets, Financial Obligations Of Elected Persons And Certain Public Officials",

Public Officials" did not refer to the previous law for data protection Law no.8517/1999 "On the protection of personal data". This cased a legal debate that culminated with the Decision No.16, date 11.11.2004 of the Constitutional Court [91] that interpreted that even the financial data was classified as a data with private character under the protection of Article 35 of the Constitution of Republic of Albania, however could not be treated at the same level with sensitive data, far more when the individual is vested with state power. In a democratic state such as Albania the transparency with the public plays a main role that could not get neglected. This being the reason why the publication of the financial assets is not considered as a breach on the private life. [92]

Subsequent to the consent LPDP envisages other interlinked right of the data subjects such as the right of access. Article 12 LPDP states that data subjects have the right to receive confirmation from the controller as to whether or not personal data concerning them are being processed, as well as access to the personal data and information about the processing if this is the case. If by the access data subjects assess incorrect information, preceding the Article 13 LPDP, they have the right to rectification, meaning that they ask for their personal data that is incorrect to be corrected by the controller as soon as possible. In some circumstances, such as when the personal data are no longer required for the purposes for which they were collected, preceding the Article 13 data subjects have the right to demand from the controller the erasure of personal data about them without undue delay. This right is envisaged as the right to erasure. Another scenario might be if the subject simply does not wish the processing of a correct data so the Article 15 gives the latter the right to refuse processing of his data and either request for the controller not to start processing the data, stop processing of the data or request permission before the starting of processing of the data.

If the data subject in exercising his/her rights has seen irregularities from the controller or processor and thinks that his/her personal data is violated Article 16 of the LPDP reserves the right to complain. Consequently every individual or data subject has the right to issue a complaint to the administrative body assigned by law to investigate and issue administrative

[91] Constitutional Court of the Republic of Albania. (2004). Decision No. 16, date 11.11.2004.
[92] Ibid 77, pg.138.

sanctions regarding data violations, which in this case is the Commissioner for the Data Protection and the Right of Information. The data subject, after issuing a complaint by the Commissioner as an administrative body has the right to issue a claim to the court as well.

Regarding the Commissioner for the Data Protection, LDPD provides the legal foundation for the role and responsibilities of the Commissioner for Personal Data Protection (CPDP) in Albania. The Commissioner for the Data Protection is established under Article 29 of the LPDP as an independent administrative entity charged for supervising and enforcing LPDP compliance, increasing knowledge of data protection rights and obligations, and giving guidance and assistance to controllers, processors, and data subjects. Consequently the CPDP plays a crucial role in ensuring the protection of personal data and is the most important entity in Albania for data protection.[93] As a result Article 30 and 31 of the LPDP defines the CPDP's functions and responsibilities, which are included within a brief analysis below.

Firstly CPDP is assigned to tasks of monitoring and enforcement. According to Article 30/a/b) the CPDP is in charge of monitoring how closely controllers and processors adhere to the LPDP by conducting administrative investigations, ordering erasing of the data and imposing administrative fines and other sanctions. Consequently, the CPDP offers controllers, processors, and data subject's advice and guidance on how to apply the LPDP, including advice on data protection impact analyses and data processing agreements. This is a complementary role of advice and guidance envisaged in Article 30/c. In order to ensure that data protection laws are consistently applied internationally, the CPDP collaborates and coordinates with other supervisory bodies, both in Albania and abroad. This is classified as cooperation and coordination function envisaged in Article 31 i/j. The main role and function of the CPDP is to receive and look into complaints and disputes about the handling of personal data, and it may take appropriate action to address these problems as envisaged in Article 31/ ë. Furthermore CPDP has some responsibilities regarding the future violations that go hand to hand with the preventive role. As such Article 31/f of LPDP encompasses that the CPDP is in charge of approving impact analyses on data protection for processing operations that pose a significant danger to the rights and liberties of data subjects. Lastly but not the least is the function of raising awareness. According to Article 31 ç)/h the CPDP works to increase the

[93]DLA Piper. (2023). Data Protection Laws in Albania.

public's understanding of their rights and responsibilities with regard to data protection, including by publishing policies, instructional materials, and guidelines. In my opinion this function is very accurate and significant in the Albanian's situation since Albania has low level of legal awareness in general. [94]

In addition to the rights of data subjects, after the right to complain to the Commissioner, the right to compensation is another mentioned in the law of 2008 on data protection, precisely Article 17. This right encompasses that the data subject that has suffered a violation of data protection has the right to be compensated for that damage accordingly.

Regarding the duties of the controllers there are some main duties envisaged in the law such as the obligation to inform in the Article 18, which expresses the obligation to inform the data subject about the processing of the data as well as the obligation to erase and rectify the data and sufficient data for the aim of the storing (Article 19 LPDP).

2.3 Comparative analysis between EU "*acquis*" and Albanian legal framework

Albania began negotiations on a Stabilization and Association Agreement (SAA) in 2003, after being officially recognized by the EU as a "potential candidate country" in 2000. This was agreed upon and signed on June 12, 2006, completing the first significant step toward Albania's full membership in the EU. [95]Albania submitted a membership application to the EU in April 2009, and in June 2014, it was given candidate status. [96] Therefore, Albania is a potential European Union member that is part of the future enlargement agenda of European Union. In July 2022, Albania and the EU together convened their first intergovernmental conference. [97] The formal commencement of negotiations was on July 19, 2022. [98] One of the most important conditions to be fulfilled in the legal field envisaged by the Copenhagen Criteria [99]is the compliance with the European Union "*acquis communautaire*" and 35 Chapters; therefore the compliance with the GDPR "*acquis*" and harmonization of the

[94] United Nations Development Program. (2018). For a more Accessible Justice for Albanian Men and Women.
[95] EUR – Lex. (2019). Stabilization and Association Agreement with Albania. Summary.
[96] European Council, Council of European Union. (2023). EU Enlargement Policy, Albania.
[97] Radio Free Europe / Radio Liberty. (2020). "EU Leaders Give Final OK To Begin North Macedonia, Albania Membership Talks".
[98] Casert, R. (2022). "EU starts membership talks with Albania, North Macedonia", Associated Press.
[99] EUR – Lex (2021) Accession Criteria, Copenhagen Criteria.

Regulation with the Albanian Law is a "must". [100] In accordance with Article 79 of the Stabilization and Association Agreement, Albania will align its personal data protection laws with Community law as well as other European and international privacy laws.

To comply with the EU "*acquis*" on data protection, Albanian law has been continuously updated. As mentioned above, the majority of international data protection regulations, notably the Council of Europe Convention for the Protection of Individuals with respect to Automatic Processing of Personal Data, have been approved by Albania. The 2018 Protocol amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data was accepted in principle by a Decision of the Council of Ministers in December 2020, opening the way for its signature. [101] The required protection of personal data is provided by Albanian law No.9887/2008 (amended), which is strengthened by secondary legislation passed by the Council of Ministers and the Commissioner. [102]

In details, if we have to compare the first source of EU "*acquis*" which is Article 16 of TFEU[103] Albania is fully aligned with Article 16 of TFEU and Article 8 of the Charter of Fundamental Rights because of the Article 35 of the Constitution of the Republic of Albania, principles expressed in Article 5 of the LPDP and Article 29 of LPDP with the appointment of the Commissioner. [104]The other source of EU "*acquis*" regarding data protection is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.[105] The level of the Albanian legislative framework's compliance with Regulation 2016/679/EU on the protection of personal data has not been evaluated. This analysis will be done as part of the Standard

[100] Ministry of Justice. (2022). Assessment for the Draft Law for the Protection of Personal Data, Electronic Registry for Public Announcements and Consultation, pg.2.
[101] Albanian Ministry of Foreign Affairs, (2021). Legal gap assessment (16/17) Chapter 23: Protection of personal data.
[102] Zotaj, S. (2021). "Protection on the Personal Data in Albania in compliance with the General Data Protection Regulation", pg 3.
[103] European Union (2008) Treaty on the Functioning of the European Union (TFEU): Article 16 Official Journal C 115, 9/05/2008. p.47.
[104] Ibid 99.
[105] European Union. (2016). Regulation (EU) 2016/679 of The European Parliament And of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Twining Project, which is scheduled to begin in 2020. [106] However, as assessed by this legal gap assessment that Albanian legislation is *partially aligned* with the Regulation. In my opinion this is expectable because Albania is on the way to becoming a member of EU and complying with the Regulation in the same level as being a Member State.

Convention (No. 108) for the Protection of Individuals with regard to Automatic Processing of Personal Data is another important source of EU acquis and Albania is *fully aligned* with it since Albania has ratified it [107]

From the legal gap assessment on "*aquis*" of Chapter 23 in 2021 is concluded that parts of Albanian law are mostly in line with EU acquis. However, it is laid down that in order to completely reconcile the General Data Protection Regulation 2016/679 and the Police Directive 2016/680, it is necessary to continue efforts to connect the personal data protection legislation with those two pieces of legislation. [108]

2.4 Comparative analysis regarding GDPR and LPDP

The Albanian Law on Personal Data Protection and the European Union's (EU) General Data Protection Regulation (GDPR) have certain parallels in terms of scope, data subjects' rights, data protection officers, and data breaches. However, the two legal frameworks have significant differences, particularly in terms of territorial scope, penalties, consent, and data protection impact assessments (DPIAs). [109]

GDPR is only one Regulation that actually embodies the whole corpus of legal base used in cases of data violation, while in Albania a series of other laws and bylaws are directly or indirectly engaged for the protection of the right to privacy and data protection, such as decisions, instructions and legal acts of the Commissioner of Data Protection.[110]

2.4.1 Rights of Data Subjects (Right to Data Portability and Right to Be Forgotten)

[106] Ibid 99, pg.21.
[107] Ibid 84.
[108] Ibid 99, pg.6.
[109] Ibid 100.
[110] Ibid 77.

Regarding the rights of data subjects specified in the Article 20, there is an additional principle incorporated in the GDPR such as the right to data portability, which allows individuals to receive their personal data in a structured, commonly used, and machine-readable format when they request it online or in order to transmit that current data to another controller. [111] Article 12/a of the LPDP envisages the right to access stipulating that data subjects have the right to receive confirmation from the data controller as to whether data pertaining to them is being processed, and if so, access to that data. Even though LPDP envisages the right to access in Article 12 LPDP, it does not specifically provide for data portability which is an absent right for the citizens of Albania and if added, would facilitate the transferability of data for data subjects.

Another novelty added to the GDPR regarding the rights of data subjects is the right to be forgotten.[112] This concept emphasizes the right of an individual to request the erasure of his data and their removal in case they are incorrect or if the time and purpose of using that data has ceased to exist. In the Albanian law the only provision that can be parallelized and interpreted as right to be forgotten in the case of removal of incorrect information is the Article 13/1 of LPDP, "The right to request correction and erasure". However Article 13 GDPR provides for the right to erasure and imposes particular duties on data controllers, such as disclosing to data subjects the categories of personal data that are processed and the purpose of the processing (Article 13 GDPR). Consequently Article 13/1 LPDP is harmonized with Article 13 GDPR but not with Article 17 GDPR that specifies the right to be forgotten. Thus, it is implied that Albania must add this new dimension of data protection in details and specify the cases when this right should be exercised. This should be done for the purpose of defining clearly its limits, clarifying the balance between the right to be forgotten and the right to be informed. [113]

2.4.2 Territorial Scope

Regarding the scope expressed in Article 51 GDPR and Article 4 LPDP there are a lot of similarities that are attributed to the territorial jurisdiction of the respective laws. The GDPR,

[111] Ibid 49.
[112] Article 17 GDPR
[113] Ibid 100, pg VII.

however, has a wider geographic scope than the Albanian law, which constitutes what is called a difference in territorial scope. [114] Regardless of where the controller or processor is based, the GDPR applies to all data controllers and processors that handle the personal information of EU citizens. [115][116][117]The Albanian law, on the other hand, is applicable to foreigners exercising their activity in Albanian but does not provide for controllers that are established out of the territory of the Republic of Albania. [118] If Albanian law expands the scope of this law it would grant a higher protection to the Albanian citizens not limited to the actual headquarters of the origin of a certain legal entity.

2.4.3 The Right to Consent

The consent is the main aspect that is embodied in the data protection principles but there is a significant difference regarding some elements of the consent of GDPR and LPDP. Article 7 GDPR requires data controllers to get data subjects' explicit and informed consent before processing their personal data while Albanian legislation simply demands "consent". Article 3/12 and Article 6/1/a in its simple term which is not defined and may be less severe than the GDPR's requirement for explicit and informed consent. An example regarding consent is the provision of Article 14 (2) (f) GDPR that requires consent even in cases where the actual data is already public. On the other hand, the Albanian law does not provide for such a specific criterion, implying in the Article 6 (3) of the LPDP [119]that if the data is already public the controller or processor has automatically obtained the consent to store and use [120]it for the purpose of enhancing business opportunities.[121][122] In my perception this provision has a tremendously important value because it is the cause of a lot of violations and leaves spaces

[114] Ibid 49.
[115] "The Territorial Scope", Article 3, The General Data Protection Regulation, 2016
[116] Sorensen J., Kosta S., (2019). "Before and after GDPR: The changes in third party presence at public and private European websites".
[117] Ch. J., Hoofnagle, B. Sloot, F. Borgesius. (2019). The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, Vol 28, No.1, 65-98.
[118] Ibid 100, pg. 3.
[119] "The controller or processor, dealing with the processing of personal data, in order to provide business opportunities or services, may use personal data for this purpose obtained from public data lists.
The controller or the processor cannot continue the further processing of the data specified in this paragraph, if the data subject has expressed disagreement or objected to their further processing. No additional personal data can be linked to the data specified above, without the consent of the data subject."
[120] Article 6 (3 of the LPDP.
[121] Article 6 (3) supra
[122] Ibid 100, pg.6.

for grey zones in implementation. However, it is underlined that Article 6(3) of the LPDP interprets that the data taken from public list means the data taken from public institutions and no other available information that are easily found online. [123]

2.4.4 Obligation of the controller (accountability principle)

One of the innovations of the Regulation is related to the provision of the controller's accountability, which passes the proof of burden to the controller for complying with the Regulation (Article 30 GDPR).[124] The Regulation requires controllers to demonstrate compliance, among other things, with the following provisions: a) obtaining approval (when necessary), in accordance with Article 7(1); b) rejecting the request of the data subject for the exercise of the right to access or correction of data (Articles 11(2) and 12(5); and c) failing to respect the data subject's right to object to processing (Articles 21(1). [125] Although Albanian law expressly recognizes that controllers must implement its requirements through automatic processing or other methods in the Article 5/2 LPDP it never specifically calls for the controller to provide evidence of compliance with the law, unless the Commissioner or even the court so requests. As a result, by the analysis of the Albanian Helsinki Committee it is essential that the Albanian law adhere to the same regime in this regard and recognize the controllers' responsibility for upholding all legal requirements, rather than just the requirement to document the technical-organizational measures as per Article 27(2/1) of the LPDP, and place the burden of proof on them. [126]

Furthermore, in the GDPR the controller has the obligation to document any processing activity,[127] while in Albanian law the Article 21 LPDP requires for the controller to notify the Commissioner before starting the processing, which is not completely in line with implementing powers of the Commissioner because of the huge number of controllers that might notify at the same time. Due to this, the Regulation altered the method, dodging the notification process and requiring controllers to maintain data resembling financial accounts

[123] Ibid 100, pg 7.
[124] Ibid 68, pg.34
[125] Korff , Georges, M. (2019). The DPO book.
[126] Ibid 68.
[127] Guidelines 07/2020 on the concepts of controller and processor in the GDPR, pg 8.

for all processing activity,[128] a change that would improve the Albanian regulatory norm regarding the accountability principle.

Article 25 (1) GDPR introduced a novelty in order to adapt the protective infrastructure to the technological developments the requirement to incorporate protection through data protection "by design" and "protection default" into the technological design of services.[129] This right requires controllers to show compliance with the GDPR and to establish adequate technical and organizational means to ensure the protection of personal data.

GDPR envisages in the Articles 37 – 39 the role of Data Protection Officer (DPO), which is an independent structure aiming at supervising and controlling the data processing activities of the public authorities. [130]In order to achieve a greater degree of enforcement of the standards for the protection of personal data, it is important that our legislation on the protection of personal data define such a structure to the controllers. The creation of guides to help DPO's as well as legal training for staff members will be necessary to fulfill this new responsibility for the controller.[131]

2.4.5. The Commissioner

GDPR envisages in the article 58 - 2/1 the requirement that an independent entity should monitor and protect the personal data in national level. In the Albanian legal framework, that institution is presented by the Commissioner for the Protection of Information and Data Protection.

"Data protection Commissioner" is the main institution appointed by the Albanian law to govern breaches of the right to privacy. Article 31 LPDP envisaged the right to issue *"ex officio*" investigations, issue recommendation and undertake administrative sanctions as the main functions of the IDP.

The process for issuing administrative fines is another distinctive function. In accordance with GDPR, supervisory authorities have the authority to punish data controllers and processors

[128] Ibid 115.
[129] Ibid 68, pg.35.
[130] A data protection officer is required to be appointed in all public authorities or bodies (except courts acting in their judicial capacity).
[131] Ibid 68, pg.36

following an inquiry and an opportunity for them to be heard. (Article 51 GDPR) In contrast, the imposition of fines under the Albanian Data Protection Law is subject to the Commissioner for Data Protection's decision, which is subject to appeal before the Administrative Court (Article 28). Consequently, it is implied that the Commissioner in the Albanian law is the equivalent of the supervisory authority set out in the GDPR.

The Commissioner amongst other rights has the authority to issue certain decisions and recommendations to particular sectors in accordance with the law on the protection of personal data that constitute another secondary source of law. Specifically we can mention; Commissioners' decision no.2, Commissioners' decision no. 6, Commissioners' decision no. 8, Instruction no.3 clarifies the processing of personal data in CCTV surveillance and so on.[132]

However, a critic has been evaluated because the law "On the Protection of Personal Data" places a severe burden on the Commissioner, giving him the responsibility of ensuring that the activity of controllers and processors complies with the legal requirements. Because there are so many controllers and processors in both the public and private sectors and because the Commissioner's office has severe limitations of both technical and human resources, it is practically impossible to achieve this competency. [133]

Penalties

Regarding penalties administrative fines are provided as a mechanism of enforcing data protection standards in both the GDPR and the Albanian Data Protection Law. The penalties under GDPR are envisaged in the Article 83. Even though the general provisions and level of fines is envisaged here the assessment and implementation is left to be evaluated case by case by the national authorities of the European Union Member States. [134] Under the GDPR there are 2 levels of fines recognized;

The first level fines vary from 10 000 000 Euro up to 2% of the company's annual revenue (Article 83/4).

The second level fines vary from 20 000 000 Euro up to 4% of the company's annual revenue. (Article 83/5)

[132] Ibid 99, pg 9-10.
[133] Ibid 68, pg.8.
[134] Recital 79 of the GDPR and Article 83/9 of GDPR.

According to the Albanian legal system, the lowest level of fines is reportedly 10 000 ALL and is imposed when data controllers use personal data in violation of Chapter II of the Law "Processing of Personal Data", while the highest level of administrative fines is reportedly 50 000 ALL and is imposed when data controllers fail to comply with their duty to notify the subject as defined in Article 39 of this Law. [135] This comparison sets out the difference that Albanian fines permitted are relatively low in contrast to GDPR. While the development of the nation can influence the level of fines, there is a significant difference between the levels in the EU and Albania. There reason why GDPR envisages high fines is in order to highly protect the data and is in proportion with the turnover that these companies might have from the gains of using data in contrary to the Regulation. Moreover, the regime of fines provided by the current law does not it turns out to be effective. [136] Otherwise, even Albanian law should raise its fines in order to raise awareness for the importance of data protection. [137]

[135] Law no. 9887, date 10.03.2008 Personal Data Protection, Albanian Law.
[136] Ibid 68, pg.9.
[137] Ibid 100, pg. 23.

CHAPTER III: SERIOUS DATA BREACHES IN ALBANIA

3.1 Premise

The right to privacy constitutes the right of any individual's information to be confidential, carefully accessed, stored and destroyed. Albania is entitled to all its obligations regarding protecting the privacy of individuals and has done so by the implementation of the Law 9887/2003 (amended) of the Data Protection and the decisions displayed by the Commissioner for the Data Protection. However, some last events have caused major distress regarding this right for various leaks have resulted in massive dissemination of personal information. This part of the thesis will display the cases of leaks; show how the Commissioner has reacted towards them through administrative investigation and how the Prosecutors' office has reacted through criminal investigation.[138]

3.2 Chronological order and the facts of the Leaks

The first leak happened on April 2021, where the Tirana's voter's entire database was leaked containing all the personal information of 2,070,000 citizens.[139] They held respectively their name, surname, date of birth, identity card number and their home addresses as well as their political convictions. The database provided even comments sections where sensitive information [140] such as religion, and family situation was displayed. The database contained political information and was suspected to have been owned by the political party in power.[141]

The second leak happened on 22 December of 2021, only 9 months after the first leak. 630,000 employees' salaries were leaked breaching the confidentiality of the salary. [142],

---

[138] The Procedural Criminal Code of the Republic of Albania (2017) SBN 978-9928-01-073-5.
[139] Commissioner for the Right to Information and Data Protection. (2021). Recommendation No. 44, 19 August 2021, "On the controller "Socialist Party of Albania".
[140] According to the Article 3 (4)of the LPDP sensitive data is any information about the natural person, related to his origin, racial or ethnic, political opinions, trade union membership, belief, religious or philosophical, criminal conviction, as well as data about health and sex life.
[141] A. ,Taylor. (16 April 2021). "The Leak of Over 910,000 Albanians Personal Data to Politicians and the Public, Exit News".
[142] Commissioner for the right to information and the protection of personal data. (2022). Decision of the Commissioner No.52, date 24.11.2022, "For the Controller "National Tax Directorate".

The third leak happened on 24 December 2021 where 530,452 license plates of the cars altogether with the credentials of the owner and other detailed information of the vehicle were disseminated. [143]

The fourth event was a cyber – attack that happened on September 2022 by alleged external forces of Iran that gained access of all the Albanian governmental systems (e- Albania and TIMS). This attack breached the right to privacy and threatened the area of cyber security and e-governance.[144] This caused for all the systems to shut down for days and big queues created in the borders became problematic because of the manual registration of people. The state institutions were completely paralyzed once again causing distrust, fear, disorganization and financial loss more than ever.

As shown above, these leaks and the last cyber-attack happened during a period of 2 years. These leaks posed a serious threat to the data protection rights of Albanian citizens exposing nearly all the personal information, going more into the depth of sensitive data, for which in the Article 24/1/a, Law 9887/2008 (amended) on the Data Protection is required special permission from the Commissioner to store and process this kind of data. The leaks showed in principle not only the violation of the Article 27 of the LPDP for the storing of the data and ensuring the cyber security of those data in order to prevent them from being retrieved by the third parties, but even for the breaches of the first phase of the "consent" which was given to process all those data.

3.3 First leak

Regarding the first leak, the database showed information of a patron that was put for political purposes to collect political information regarding respective people they were assigned and report that information which was then stored at the database. It was eluded that the political party in power created the database and aimed to use it in order to influence the voting's.[145] On April 16 and April 19, 2021, the Commissioner sent letters to Authority of the Electronic

[143] Commissioner for the right to information and the protection of personal data. (2022). Decision of the Commissioner No.51, date 24.11.2022, "For the Controller "General Directorate of Road Transport Service".
[144]Sinoruka, F. 2022). Massive Data Leaks in Albania Pose Public Security Question, Balkan Insight.
[145] Ibid 137.

and Postal Communications (AKEP) and the General Directorate of State Police requesting their immediate blocking and the beginning of legal proceedings against the individuals who own/own these webpages. [146] On April 19, 2021, the Commissioner ordered an administrative investigation into the accountable institutions that had access to part of these data. Albanian Helsinki Committee [147]observes that this inquiry has started out with an oblique report from a chronological point of view, harming the effectiveness over time and in a thorough manner. [148]

To be more concrete, the Commissioner which based on the Article 3/1/a of the Law 9887/2008 has the duty to make assessment regarding this field and issue "ex officio" investigations held that there was no sufficient evidence that proved that the party in power created the database or that the information was secured from state databases. It comes out that the administrative inquiry for the voter database against the controlled electoral entity and public institutions has only been lightly and incompletely developed. The assessment of Albanian Helsinki Committee held that the commissioner had legal options available to him, but he chose not to use them by not requesting a wider range of material proof that would have allowed him to clarify the incident and specifically identify the controllers' liability. The only active action of the Commissioner was the issue of the Recommendation no.44 giving recommendation to the party in power in order to meet higher standards of data protection.[149]

Another problem insinuated is that the citizens did not raise their voice as much as expected. Regarding the Article 16 of the LPDP the individuals have the right to issue a complaint to the Commissioner when they think their personal data is being violated. Regarding this leak the Commissioner's Office states that between April and August 2021, it received 81 complaints on the legality of the handling of voters' and residents' personal data. [150] This without a doubt insinuates a significantly small number of individuals out of 2,070,000 citizens, indicating a considerate problem regarding the awareness of data protection amongst Albanian citizens.

Another issue that is fit to point out is the use of international mechanisms as a way of protecting the right to privacy in this context. Since Albania has ratified the ECHR, its citizens

[146] Ibid 68, pg.10.
[147] NGO in Albania, Branch of Helsinki Committee.
[148] Ibid 68, pg.10.
[149] Ibid 137.
[150] Ibid 68, pg.11.

have the right to submit claims in ECHR regarding the breaches of fundamental rights from the state. Deductively, in the cases of suspected violations of human rights the citizens can issue claims in the European Court of Human Rights. No claim was submitted to the ECHR by any Albanian citizen regarding these breaches of personal data; therefore we do not possess an assessment from the European Court of Human Rights regarding the cases. However, there has been a parallel assessment of the ECHR Judgment of Spain in 2022 [151] and the current leak in Albania. The facts of the case were that the Police of Spain had created a database with 20 Spanish judges' personal information despite them never being connected to crime. In 2014 where some judges wrote down an article regarding the independence of Cataluña, the journal published photos and personal information of 20 judges, accessed from the police database. The ECHR held that the police did not have the right to access these information since the judges were not related to crime and violated their right to privacy altogether with the journal, while the government was responsible for the breach of the right to privacy because it did not prevent it. This decision of ECHR expressly confirmed that the State has an obligation to actively protect the individual from arbitrary interference with their privacy. Consequently is interpreted that the Albanian government breached Article 8 of ECHR by compiling personal information without a legitimate purpose and with allowing it to be leaked altogether with the ineptness to not find the concrete perpetrators but leaving the case to fade away. [152]

3.4 Second leak

Furthermore, in the 22 December of 2021, 630,000 employees' salaries were leaked. [153]Since any information that relates to an identified or recognizable individual is referred to as personal data and any data that can directly or indirectly identify a person, such as their name, identification number, contact information, or any other information that is particular to their identity, falls under this category[154], it is logically concluded that the salary of an individual constitutes a private information that falls under the protection of personal data. This implies that this leak breaches the confidentiality of the salary of the individuals and constitutes a violation. The data was originally stored in the National Tax Directorate and was later proven

[151] European Court of Human Rights. (2022). Case of M.D and others v. Spain. (Application no. 36584/17).
[152]Exit News. (2022). "ECHR Ruling in Privacy Case Shows Similarities to Albania's Massive Data Leak".
[153] Ibid 140.
[154] Article 3/1 of the Law 9887/2006 on the Data Protection.

by the Commissioner that was leaked by two internal employees of the Directorate, who were eventually arrested.[155] [156] In this case the phase of processing this information by the state institutions is lawful, meeting the legitimate purpose of the storing but the breach occurs in the moment of the leak of this information, creating problems with the security of such data, training of the staff on how to store them and prevention of the information from being accessible to non-authorized sources, more precisely alignment with Article 27 LPDP. The Decision of the Commissioner No.52, date 24.11.2022 [157] found the National Tax Directorate in the breach of personal data and fined the controller with 25.000 Euro.

In this case it is concluded that the Commissioner exercised his responsibility to issue investigations after a breach has occurred, deeming this function to be fulfilled by CPDP. The only thing that should be deduced is that the Commissioner is the highest institution for the protection of personal data and should be given more sources in order to fulfill its obligations relating to "preventing" mechanisms and issuing random and periodic control over the institutions as set out in previous paragraphs on the role of the Commissioner. The annual report from 2021 shows that The Commissioner's human resources are lacking, which further supports the lack of personnel statement.[158]

3.5 Third leak

In the 24 December of 2022, only two days after the second leak, another leak followed where 530,452 license plates of the cars altogether with the credentials of the owner and other detailed information of the vehicle were disseminated.[159] Administrative investigation by the Commissioner showed that the information for the leaks was obtained from the government institutions precisely General Directorate of Road and Transport (DPSHTRR) which were responsible to store and protect the personal data according to the law but apparently failed to do so. The Law "No. 9887 "On the Protection of Personal Data" in the Article 5 states that the processing of the data should be legitimate and proportional to the aim of accessing by the

[155] Bogdani, A. (21 February 2022). The unsafely of personal data threatens Albania's 'digital governance', Reporter.al.
[156] Article 122 of the Criminal Code of the Republic of Albania.
[157] Ibid 140.
[158] Annual Report of the Commissioner of the Right to Information and data Protection pg. 47. – as cited by Albanian Helsinki Committee Report, pg 38.
[159] Ibid 142.

institution. In our last cases the information was accessed by government that had gathered it legitimately, but was not in compliance with properly storing them. The Decision of the Commissioner No.51, date 24.12.2022 [160] found the institution in breach and fined the latter with a fine of 8.800.00 Euros. What is concluded by this other breach is that the institutions are not properly trained. An example is the Recommendation of the Commissioner no.32, date 23/07/2022 [161] issued as an ex officio routine investigation of the Commissioner that found non- compliance of the entity regarding the training of the staff, has not notified the subjects for the processing of data, breaching Article 21 and 22 of the Law on data protection, as well as did not comply with good administration of SMSI. [162]

These situations show negligence form the authorities in order to fully comply with given laws and specifically with the obligations of Article 21 and 22 regarding the staff that is obliged to ensure the safe processing and storing of the personal data that are indirectly responsible for possible leaks. As such the staff must be trained accordingly in technology and information as well as in the specific regulations of how to process it.

Another challenge contributing to the breach of the right to privacy and the leaks in general is the education of citizens regarding this right. In relation to the illegal dissemination of the category of personal data for "employees/employees" in public and private sector and the illegal spread of the category of personal data for "owners vehicles", 47 complaints were filed in the Commissioner's Office, of which 22 were against AKSHI and 25 to the DPT. [163]It is important to point out that the processing of personal data is allowed when the citizen has given consent, which was the case in the majority of stored data. Accordingly, the processors are exempt from primal responsibility of having access. This phenomenon indicated a high level of digital illiteracy in citizens that have yet to educate themselves regarding protection of their personal data.[164] As such, this asserts that not only the lack of security and implementation of GDPR has led to these repeated violations but even the citizens themselves

[160] The Commissioner for the right to information and the protection of personal data. (2022). Decision of the Commissioner No.51, date 24.11.2022, "For the Controller "General Directorate of Road Transport Service".
[161] Recommendation of the Commissioner of the Information and Protection of Personal Data no. 32, date 2.07.2022 for the controller "Special College of Appeal".
[162] System of Management of the Security of Information
[163] Ibid 68, pg.43.
[164] The Commissioner for the Right to Information and Personal Data Protection, National Campaign "Digital Education Play &Learn – Happy online No 9 &10, December 2020.

have contributed in the breach of this right. Accordingly, a relevant solution is for the government and NGO-s to provide more information to the public regarding GDPR and the right to privacy.[165]

3.6 E- government; Cyber security and the Cyber attack

Another challenge regarding right to privacy and more specifically data protection has to do with the e- government implementation. E- government is an initiative to modernize government functioning and promote more efficiency for citizens as well. [166]

In this aspect the data protection is very much related to cyber security because it bases the actual government work and citizen's data circulating all within technological devices. At this rate some researchers have highlighted the fact that it is now appropriate to begin treating cyber security as a human rights concern due to the advancement of technology and online interactions. [167]

In this regard, the Albanian government made an effort to promote digital initiatives as a tool for modernizing governance, as well as knowledge for a more open and economically viable society for the citizens, to join regional cooperation, and in coordination with the European Law and institutions within the process of Albania's integration into the European Union.[168] Taking into consideration that Albania is a developing state, it is considered as one of the nations with the fastest-moving telecommunications and internet access. The country's economic and social development will benefit from the increased use of communication, but this rapid change puts it at risk for cyber-attacks against both state-owned entities and private players.[169]

As much as the Albanian government tried to mend the cyber security issue following the leaks it did not prove effective because the last attack was issued in September 2022 allegedly by external forces of Iran that gained access of all the Albanian governmental systems (e-

[165] Mapping Governance Institute. (2022). Cybersecurity and Human Rights in the Western Balkans.
[166] Council of Europe. (2022). E –governance.
[167] D.Brown. , A. Esterhuysen. (2021). Why cybersecurity is a human rights issue, and it is time to start treating it like one, Publisher: APCNew.
[168] D,. Pasha. (2022). E-Governance and the Importance of Personal Data Protection in Albania.,pg.1.
[169] Cumarsaide, R. , Fuinnimh & Acmhainni,. Nadurtha. (2015). Department of Communications, Energy and Natural Resources., Policy Paper on Cyber Security 2015 – 2017.

Albania and TIMS). [170] This caused for all the systems to shut down for days and big queues created in the borders became problematic because of the manual registration of people. The state institutions were completely paralyzed once again causing distrust, fear, disorganization and financial loss more than ever.

This cyber- attack raised questions regarding e-government and whether Albania had the resources to have a successful implementation of the latter. As such it is emphasized that security measures should be put in place to safeguard personal data and ensure that it is only used for approved and legal purposes[171], which did not seem as the case. A possible solution to this is for the government to hire professionals in IT and build strong detecting systems as well as endure high security in the official emails and documents of governmental institutions.

Despite these reports, it is worth analyzing the effort of the government and whether there was actually any law regarding cyber security to better understand the "positive role" of the State in preventing this attack.

Regarding this the Albania had the Law No. 2/2017 "On Cyber Security" adopted on 2017[172], which was firstly applicable for public sector later expanded to the private. The law displays measures of the cyber security in order to achieve a high level of security. Chapter II of this law displays the responsible entities in the field of cyber security, which places the "responsible authority" as the entity responsible to define cyber security measures, [173]administrates incidents [174] and acts as Computer Security Incident Response Team (CISRT)[175], which consists of computer security experts at any operator that oversees key information infrastructure[176] Article 6 of the Law on Cyber Security envisages that other entities responsible are " critical information infrastructure operators" that based on the Article 18 of this law is interpreted as the assigned IT experts on the specific institution. As stipulated from this law, Albania has a regulatory framework, however modest it is. The structures

[170] Ibid 143.
[171] Bygrave, Lee A., (1998). Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. International Journal of Law and Information Technology, Vol. 6, Issue 3, pg. 247-284.
[172] Law No.2/2017 "On the Cyber Security".
[173] Article 5 (1) (a) on the "Law in Cyber Security"
[174] Article 5 (1) (b) (c) on the "Law in Cyber Security"
[175] Article 1 (2) on the "Law in Cyber Security"
[176] Article 7(1) on the "Law in Cyber Security"

mentioned have a function to safeguard the activity of the institutions, however experts display that the structures created by this law are still in need of professionals. [177]

Besides the Law on "Cyber Security" and the challenges aforementioned it is worth mentioning the "Strategy for Cyber Security" 2021 – 2023 issued by the Defense Ministry. This new strategy aimed at creating and effectively deploying cyber security capabilities that the computer systems can ensure a secure online environment for all of their operations. This was meant to consolidate their defensive and offensive capabilities, raise awareness and professionalism, and improve their collaboration and coordination with other national and international institutions.

Action Plan that this strategy aimed at implementing were regarding:

- A separated responsibility, which implies the reasonable steps of the IT professionals in protecting the systems they are assigned. [178]However, we mentioned earlier that the challenge is to actually have a higher authority and more distinct responsibilities regarding the institutions, which in my opinion are not very well stipulated in this Strategy in accordance with the correct stipulation of the objective.
- Risk management, has to do with the priorities to support resources of cyber security activities.
- Protecting Armed Forces Values - The strategy aims the pursuance of cyber security policies that enhance individual and collective security in the Armed Forces, while maintaining the right of individuals for privacy and other fundamental values.[179] This point expressly emphasizes the respect for the right to privacy in relation to the cyber security which indicated the level of security that is aimed towards the dual protection of cyber security and data protection security.

As assessed from the legal analysis, Albania was not completely inept regarding the legal framework in dealing with cyber-attacks and cyber security, however the fact of the delayed

[177] Tomço, V. (2018). Cyber Security in Albania, experts and professionals needed. General Director of National Authority for Electronic Certification and Cyber Security. Risi Albania.

[178] Ministry of Defense of the Republic of Albania. (2020). National Strategy on the "Cyber Security" 2021 - 2023 pg.12

[179] Ibid 177, pg.12.

solution and ongoing consequences indicate that the "measures" that are stipulated in the law could not find the same efficiency in implementation. Therefore, as assessed from the ECHR's aforementioned judgment the lack of skills to prevent the leaks constitutes serious breaches of the "right to privacy".

On the other side, cyber security is not a new field only in Albania but an overall international threat, a gateway for the so called dark web and commitment of various crimes that better "cyber powered" states are not able to prevent. In order to counter argue for the fact that the state failed in ensuring its preventive role, it is necessary to take in consideration that the Strategy on "Cyber Security" highlights that it may take scientific researchers weeks, months, or even years to locate an online attacker, a timeline that might be interpreted as the decrease in the prevention schemes. However, the development of countermeasures always lags behind the rapid evolution of attacks. In particular, military targets, which will increasingly be the focus of espionage and cyber sabotage assaults, face substantial, growing threats from state backing of these attacks to national security.[180]

Facing these arguments it is assess that Albania is not the most prepared state in dealing with cyber-attacks, but we should use the principle of proportionality in this legal reasoning and assess carefully what level of protection we are requesting in relation to the threat posed. Cyber-attacks are threats that are not able to be prevented internationally therefore it might be unrealistic expecting that Albania could actually prevent this attack. The legal framework is adequate and the strategy on Cyber Security" shows the level of attention that Albanian government is putting to this issue. After the attack it is true that e – government systems were collapsed but no data leak followed from that and despite the slow response the "shutdown" act of the E-Systems was a measure to indirectly ensure the actual prevention of the data protection breaches of citizens. Improvements on ensuring a better protection and countermeasure can be certainly required.

Regarding the use of e – government being a new establishment not only in Albania but even in other states, the government should facilitate this process by providing more workshops or trainings for citizens, but increase the level of safety in cyber security. [181] Information leak

[180] Ibid 177, pg.10.
[181] Ibid 167, pg.7.

prevention and management procedures should be developed and implemented by servers of public institutions managed by AKSHI.[182]

The governments, state structures, guardians of personal data protection, computer systems, and servers that run Albania's electronic systems were responsible for the protection of privacy and human rights as evidenced by the publication of the payroll for almost 90,000 citizens.[183]

[182] Ibid 167, pg.7.
[183] Ibid 167, pg.6.

CONCLUSIONS

In order to make a comparison between the European Union acquis in data protection and Albanian law on data protection, the thesis analyzes firstly the General Data Protection Regulations. The reasons that contributed to the proposal of a General Data Protection Regulation after the Directive 1995/ 46 EC were the breaches and grey areas emerging with the development of technology, specifically in the international data transfer. Cases such as *Schrems I* and *Schrems II* marked the main problems of digital data protection and contributed to a better legal framework in this regard. In general, the Data Protection Regulation has increased the requirements placed on controllers and processors and reinforced the rights of those who are the subjects of personal data however even GDPR still has its own grey zones.

Regarding the Albanian legal framework, the law governing the data protection in Albania, Law.9887/2008 (amended) has a high level of protection in case of legal framework. Even though it has differences with GDPR, it cannot be assessed that the sole reason for breaches is the legal framework in Albania. Moreover, from the analyses is concluded that parts of Albanian law are mostly in line with EU *"acquis"* with certain parallels in terms of scope, data subjects' rights, data protection officers, and data breaches. However, the two legal frameworks have significant differences, particularly in terms of territorial scope, penalties, consent, and data protection impact assessments (DPIAs). Therefore it is necessary to continue efforts to connect the Albanian's personal data protection legislation with GDPR. [184]

Regarding 3 leaks that happened in Albania, the first one is connected with the leak of Tirana's voter's entire database, the second leak had to do with 630,000 employees' salaries leak, breaching the confidentiality of the salary, and the third one with the leak of 530,452 license plates of the cars altogether with the credentials of the owner and other detailed information of the vehicle were disseminated. These leaks posed a serious threat to the data protection rights of Albanian citizens exposing nearly all the personal information, going more into the depth of sensitive data breaches.

In these cases the Commissioner answered to the leaks by using all the necessary legal instruments, despite the first leak from which was assessed that the Commissioner could have

[184] European Commission. (2022). Albanian 2022 Report. Pg.17

exhausted more legal mechanisms to detect the perpetrators. This shows that generally the Commissioner is functional, in accordance with the Law. 9887/2008 (amended) however, this entity lacks human resources to fully implement all its functions, such as issue “ex officio” evaluations. Since the digitalization has made it harder to track the breaches there is to say that the Commissioner cannot be the only institution to monitor and prevent data breaches. In this regard Albania lacks assigned institutions that ensure its protection. Instead every institution has its own agency that deals with data protection and cyber security. Therefore, in case of leaks, institutions that legally store the same information dispute over the negligence of each other, rather than take responsibility. These situations show negligence form the authorities in order to fully comply with given laws and specifically with the obligations of Article 21 and 22 regarding the staff that is obliged to ensure the safe processing and storing of the personal data that are indirectly responsible for possible leaks. As such the staff must be trained accordingly in technology and information as well as in the specific regulations of how to process it.

Another contributing factor is a high level of digital illiteracy in Albanian citizens that have yet to educate themselves regarding protection of their personal data. As such, this asserts that not only the lack of security and implementation of GDPR has led to these repeated violations but even the citizens themselves have contributed in the breach of this right.

Another important aspect highlighted both in European Union and Albania is cyber security and the problems that the cybercrimes and E- governance poses. Some researchers have highlighted the fact that it is now appropriate to begin treating cyber security as a human rights concern due to the advancement of technology and online interactions. In Albania, a cyber-attack was issued in September 2022 allegedly by external forces of Iran that gained access of all the Albanian governmental systems (e- Albania and TIMS). This cyber- attack raised questions regarding e-government and whether Albania had the resources to have a successful implementation of the latter. When analyzing the legal framework Albania adopted the Law No. 2/2017 “On Cyber Security” on 2017 the law displays measures of the cyber security in order to achieve a high level of security. Consequently, Albania was not completely inept regarding the legal framework in dealing with cyber-attacks and cyber security however the fact of the delayed solution and ongoing consequences indicate that the “measures” that are

stipulated in the law could not find the same efficiency in implementation. A possible solution to this is for the government to hire professionals in IT and build strong detecting systems as well as endure high security in the official emails and documents of governmental institutions. Being aware of the increased value of cyber security Albania created the "Strategy for Cyber Security" 2021 – 2023" This new strategy aimed at creating and effectively deploying cyber security capabilities. This was meant to consolidate their defensive and offensive capabilities, raise awareness and professionalism, and improve their collaboration and coordination with other national and international institutions by highlighting separated responsibilities and risk management resources, all problems that were highlighted already. Improvements on ensuring a better protection and countermeasure can be certainly required, however we have to keep in account that cyber-attacks and E governance are a new area even for EU and international sphere, therefore the expectations to respond should be proportional to the threat posed. Therefore, Cyber-attacks are threats that are not able to be prevented internationally therefore it might be unrealistic expecting that Albania could actually prevent this attack. The legal framework is adequate and the strategy on Cyber Security" shows the level of attention that Albanian government is putting to this issue.

Presenting all the gaps, Albania is planning on enacting a new law "On Personal Data Protection" in June 2022 that is quite similar to the GDPR.[185] Another factor that necessitates alignment is the requirement to adhere to a global standard for the protection of personal data, particularly in relation to the transfer or circulation of that data from and to the EU, which is a crucial activity for the development of the data[186] The draft's main objective is to harmonize the Albanian law with EU *"acquis communaitaire".* The draft law promotes new additions such as the scope of law regarding the legal entities that are not established within the Republic of Albania. The "accountability principle" is enhanced, more precisely the new draft law envisages the new obligation of the Commissioner on issuing risk analysis for the protection of personal data before beginning a processing procedure, obligation to consult with the Commissioner in cases of high risk processing actions and the obligation of the controllers to incorporate protection through data protection "by design" and "protection default" into the

[185]Accordingly, The Republic of Albania's Ministry of Justice began a public consultation period a proposed law "On Personal Data Protection" in June 2022 that is similar to the GDPR
[186] Ibid 68, pg.1.

technological design of services. Regarding the rights of data subjects, it adds up the biometric and genetic data as a sensitive data, adapting more to the technology and being more aware of the processing of the biological information. Regarding the functions of the Commissioner, this new draft law envisages the transfer of the personal data without the authorization of the Commissioner in cases of the insufficient protection because it presents other elements that guarantee the protection like "Standard data protection clauses"[187]and "Binding Corporate Rules".[188] The New Draft Law on Data Protection is almost in complete harmonization with GDPR. Every legal gap that was highlighted in Chapter II (the differences between Albanian Law and GDPR) is now present, ensuring higher level of protection and adaption to the technological developments as well.

To conclude, the current Albanian legislation complies in principle and many provisions with GDPR. However, the differences diminish the Albanian's level of protection in a digitalized era, a gap that will positively be solved with the implementation of the New Draft Law that Albania will adopt.

REFERENCES

[187] Article 5/24 of the New Draft Law on Data Protection.
[188] Article 5 /25 of the New Draft Law on Data Protection.

Doctrine

Albanian Ministry of Foreign Affairs. (2021). Legal gap assessment (16/17) Chapter 23: Protection of personal data. https://integrimi-ne-be.punetejashtme.gov.al/wp-content/uploads/2022/02/NPEI_2022-2024_EN-.pdf

Albanian Helsinki Committee. (2022). "Legal and institutional overview for his protection and safety personal data in our country and their compliance with the acquis". file:///C:/Users/Saturn/Downloads/komiteti-shqiptar-i-helsinkit-dokument-politikash-dhe-qendrimesh-mbrotja-e-te-dhenave-personale.pdf

Albanian Ministry of Foreign Affairs, (2021). Legal gap assessment (16/17) Chapter 23: Protection of personal data. https://integrimi-ne-be.punetejashtme.gov.al/wp-content/uploads/2022/02/NPEI_2022-2024_EN-.pdf

Bogdani, A. (21 February 2022). The unsafely of personal data threatens Albania's 'digital governance', Reporter.al. https://www.reporter.al/2022/02/21/pasiguria-e-te-dhenave-personale-rrezikon-qeverisjen-dixhitale-te-shqiperise/

Bygrave, Lee A. (1998). Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. International Journal of Law and Information Technology, Vol. 6, Issue 3, pp. 247-284, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=915065

Ch. J., Hoofnagle, B. Sloot, F. Borgesius. (2019). The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, Vol 28, No.1, 65-98. https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501

Casert, R. (2022). "EU starts membership talks with Albania, North Macedonia", Associated Press. https://www.ctvnews.ca/world/eu-starts-membership-talks-with-albania-north-macedonia-1.5993300

Diggelmann, O., Cleis, M. N. (2014). How the right to privacy became a human right. *Human Rights Law Review*, *14*(3), 441-458, https://www.corteidh.or.cr/tablas/r33348.pdfhttps://www.corteidh.or.cr/tablas/r33348.pdf

D.Brown. , A. Esterhuysen. (2021). Why cybersecurity is a human rights issue, and it is time to start treating it like one, Publisher: APCNew https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one

D,. Pasha. (2022). E-Governance and the Importance of Personal Data Protection in Albania. https://www.dcaf.ch/sites/default/files/imce/ECA/D.Pasha-YoungFaces2022.pdf

DLA Piper. (2023). Data Protection Laws in Albania. https://www.dlapiperdataprotection.com/index.html?t=law&c=AL

Exit News. (2022). "ECHR Ruling in Privacy Case Shows Similarities to Albania's Massive Data Leak" https://exit.al/en/echr-ruling-in-privacy-case-shows-similarities-to-albanias-massive-data-leak/

European Data Protection Supervisor. (2023). The History of General Data Protection Regulation. https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Global Freedom of Expression (2021)"Schrems V. Data Protection Commissioner, Columbia University. https://globalfreedomofexpression.columbia.edu/cases/schrems-v-data-protection-commissioner/

Gellman, Barton; Poitras, Laura. (2013). "US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program". The Washington Post. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html Greenwald, G., Poitras, L. and MacAskill, E. (2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations, The Guardian, 11 September. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower surveillance

Granger, M.-P., and Irion, K. (2018). 'The right to protection of personal data: the new posterchild of European Union citizenship?' in: de Vries, S., de Waele, H., and Granger, M.-P., eds., Civil Rights and EU Citizenship (Cheltenham: Edward Elgar Pub.), DOI: 10.4337/9781788113441.00019 https://www.ivir.nl/publicaties/download/The-right-to-protection-of-personal-data-prepub.pdf Hustinx, 2013, as cited in Vogelsang, H. (2019). *An analysis of the EU data protection policy and the significance of the Maximillian Schrems case. https://essay.utwente.nl/79033/1/Bachelor%20Harpo%20Vogelsang.pdf*

Hoofnagle, Ch. (2019). The European Union data protection regulation: what it is and what it means", Information and Communications Technology Law 65. https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501

Korff , Georges, M. (2019). The DPO book. https://www.garanteprivacy.it/documents/10160/0/T4DATA-The+DPO+Handbook.pdf

Mapping Governance Institute. (2022). Cybersecurity and Human Rights in the Western Balkans. https://www.dcaf.ch/cybersecurity-and-human-rights-western-balkans-mapping-governance-and-actors

H. Miço. (2023). The right to private and family life and the need for protection against the digital environment". European Journal of Economics, Law and Social Sciences Vol. 7 No. 2. https://sciendo.com/article/10.2478/ejels-2023-0010

Omari. L, Anastasi. A. (2017). E drejta kushtetuese, Dajti 2000, Tirane ISBN: 978 99956 01 41 6

Schwartz, P. M. (1994). European data protection law and restrictions on international data flows, *L. Rev.*, *80*, 481. https://lawcat.berkeley.edu/record/1115036/files/fulltext.pdf

Riza, G. (2021). "GDPR and personal data protection in non- EU countries: Albanian case of data protection legislation", CEUR Workshop Proceedings. https://ceur-ws.org/Vol-2872/short06.pdf

Wilson, R. (2023). Data Controllers as Data Fiduciaries: Theory; Definitions and Burden of Proof *University of Colorado Law Review, Vol. 95, No. 1, 2023* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4421296

Radio Free Europe / Radio Liberty. (2020). "EU Leaders Give Final OK To Begin North Macedonia, Albania Membership Talks" https://www.rferl.org/a/eu-leaders-give-final-approval-eu-membership-talks-macedonia-albania/30512156.html

Cumarsaide, R. , Fuinnimh & Acmhainni,. Nadurtha. (2015). Department of Communications, Energy and Natural Resources., Policy Paper on Cyber Security 2015 – 2017. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_IE.pdf

Sorensen J., Kosta S., (2019). "Before and after GDPR: The changes in third party presence at public and private European websites". https://www.researchgate.net/publication/330997511_Before_and_After_GDPR_The_Changes_in_Third_Party_Presence_at_Public_and_Private_European_Websites

Sinoruka, F. (2022). Massive Data Leaks in Albania Pose Public Security Question, Balkan Insight. https://balkaninsight.com/2021/12/23/massive-data-leaks-in-albania-pose-public-security-question/

Taylor, A. (2021). "The Leak of Over 910,000 Albanians Personal Data to Politicians and the Public, Exit News". https://www.dcaf.ch/sites/default/files/publications/documents/CybersecurityHumanRightsWesternBalkans_EN_March2023.pdf

Tomço, V. (2018). Cyber Security in Albania, experts and professionals needed. General Director of National Authority for Electronic Certification and Cyber Security. Risi Albania. https://www.risialbania.al/cyber-security-a-vital-reality-in-search-of-field-professionals/?lang=en

United Nations Development Program. (2018). For a more Accessible Justice for Albanian Men and Women. https://www.undp.org/albania/projects/more-accessible-justice-albanian-women-and-men

Vogelsang, H. (2019). An analysis of the EU data protection policy and the significance of the Maximillian Schrems case.https://essay.utwente.nl/79033/1/Bachelor%20Harpo%20Vogelsang.pdf

Weiss, Archick, (2016). U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, Congressional Research https://sgp.fas.org/crs/misc/R44257.pdf

Zotaj, S. (2021). "Protection on the Personal Data in Albania in compliance with the General Data Protection Regulation". https://www.etd.ceu.edu/2021/zotaj_sara.pdf

Legal Acts

Council of Europe, (1950), European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13, and 16. https://www.echr.coe.int/Documents/Convention_ENG.pdf

Council of Europe, (1981) European Treaty Series - No. 108,Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. https://rm.coe.int/1680078b37

Constitutional Court of the Republic of Albania. (2004). Decision No. 16, date 11.11.2004 https://www.gjk.gov.al/include_php/previewdoc.php?id_kerkesa_vendimi=513&nr_vendim=1

Directive 1995/ 46 EC. Directive (EC) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

Directive 1995/ 46 EC. Directive (EC) 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

EUR-Lex. (2014). Summaries of EU Legislation "Protection of Personal Data". https://eur-lex.europa.eu/EN/legal-content/summary/protection-of-personal-data.html#:~:text=Directive%2095%2F46%2FEC%20is,the%20European%20Union%20(EU)

European Union (2008) Treaty on the Functioning of the European Union (TFEU): Article 16 Official Journal C 115, 9/05/2008 p.47. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

European Union. (2016). Regulation (EU) 2016/679 of The European Parliament And of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Court of Human Rights. (2022). Guide on Article 8 of the European Convention on Human Rights. https://www.echr.coe.int/documents/guide_art_8_eng.pdf

European Commission. (2020). Communication From The Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European Strategy For Data".https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0066

European Commission. (2021) Albania 2021 Report. Directorate-General for Neighborhood and Enlargement Negotiations. https://neighbourhood-enlargement.ec.europa.eu/system/files/2021-10/Albania-Report-2021.pdf

European Commission. (2022). Albanian Report 2022 https://neighbourhood-enlargement.ec.europa.eu/system/files/2022-10/Albania%20Report%202022.pdf

European Parliament. (2017). The EU as a community of law Overview of the role of law in the Union, Briefing, Think Tank. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2017)599364

European Council, Council of European Union (2023) EU Enlargement Policy, Albaniahttps://www.consilium.europa.eu/en/policies/enlargement/albania/

EUR – Lex. (2019). Stabilization and Association Agreement with Albania. summary https://eur-lex.europa.eu/EN/legal-content/summary/stabilisation-and-association-agreement-with-albania.html

EUR – Lex. (2021). Accession Criteria, Copenhagen Criteria. https://eur-lex.europa.eu/EN/legal-content/glossary/accession-criteria-copenhagen-criteria.html

International Commissioner's Office. (2023). A guide to the data Protection. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

European Data Protection Board. (2016). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf

On the ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Law of 2004, Pub. L. No. 9288/2004. https://bfiniq.gov.al/wp-content/uploads/2018/06/ligji_9288_koventa.pdf

On the Protection of Personal Data, Law of 1999, Pub. L. No. 8517/1999. http://www.aac.gov.al/wp-content/uploads/2017/04/13.LIGJ-NR.8517-DATE-22.07.1999.pdf

On the Protection of Personal Data, Law of 2008, Pub. L. No. 9887/2008, as amended. https://www.idp.al/wpcontent/uploads/2020/03/Ligj_Nr.9887_dat%C3%AB_10.3.2008_i_ndryshuar.pdf

Law No. 9049, dated 10 April 2003 "On The Declaration And Audit Of Assets, Financial Obligations Of Elected Persons And Certain Public Officials", https://www.ildkpki.al/wp-content/uploads/2019/02/Law-9049.pdf.

Law No.2/2017 "On the Cyber Security" https://cesk.gov.al/wp-content/uploads/2020/07/Ligji-_Per_Sigurine_Kibernetike_Nr_2_Date_26.1.2017.pdf

The Procedural Criminal Code of the Republic of Albania (2017) SBN 978-9928-01-073-5 https://www.pp.gov.al/rc/doc/kodi_i_procedures_penale_28_07_2017_1367_5285.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council, (27 April 2016), General Data Protection Regulation (GDPR), Official Journal of the European Union, L 119/1. https://eur-lex.europa.eu/eli/reg/2016/679/ojhttps://eur-lex.europa.eu/eli/reg/2016/679/oj

United Nations General Assembly. (1948). "Universal Declaration of Human Rights" 217 (III)A. https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations General Assembly. (1966) International Covenant on Civil and Political Rights, Treaty Series, vol. 999, p. 171. https://www.refworld.org/docid/3ae6b3aa0.html

United Nations Human Rights Treaty Bodies. UN Treaty Database. https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CCPR&Lang=en

Council of Europe. (2022). Chart of signatures and ratifications of Treaty 185. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Ministry of Defense of the Republic of Albania. (2020). National Strategy on the "Cyber Security" 2021 - 2023 https://www.mod.gov.al/images/PDF/2020/Strategjia-Mbrojtjen-Kibernetike-2021-2023.pdf pg.12

Ministry of Justice. (2022). Assessment for the Draft Law for the Protection of Personal Data, Electronic Registry for Public Announcements and Consultation, https://konsultimipublik.gov.al/Konsultime/Detaje/472

The Commissioner for the Right to Information and Data Protection. (2021). Recommendation No. 44, 19 August 2021, "On the controller "Socialist Party of Albania". https://www.idp.al/wp-content/uploads/2021/08/rekomandimi_nr_44_pssh_2021_dmdp.pdf

The Commissioner for the right to information and the protection of personal data. (2022). Decision of the Commissioner No.52, date 24.11.2022, "For the Controller "National Tax Directorate". https://www.idp.al/wp-content/uploads/2022/11/Vendim-TATIME.pdf.

The Commissioner for the right to information and the protection of personal data. (2022). Decision of the Commissioner No.51, date 24.11.2022, "For the Controller "General Directorate of Road Transport Service". Retrieved from https://www.idp.al/wp-content/uploads/2022/01/Vendim-DPSHTRR.pdf

Council of Europe (2004) E -governance https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Default_en.asp

Caselaw

European Court of Human Rights, Case of Denisov v. Ukraine (25 September 2018), Strasbourg Application no. 76639/11 http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-186216%22]}

European Court of Human Rights, Case of Bărbulescu v. Romania (5 September 2017), Strasbourg, (Application no. 61496/08) http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-177082%22]}

European Court of Human Rights, Case of Botta v. Italy (24 February 1998), Strasbourg, (153/1996/772/973) http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58140%22]}

European Court of Human Rights, Case of Axel Springer AG v. Germany (7 February, 2012), Strasbourg,(Application no. 39954/08) http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-109034%22]}

European Court of Justice, Rechnungshof vs. Osterreichischer Rundfunk, C-465/00, C138-/01, and C-139/01 [2003], ECLI:EU:C:2003:294 https://eur-lex.europa.eu/legal content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2003%3A294

European Court of Justice, Bodil Lindqvist v Åklagarkammaren i Jönköping, C-101/01 – [2003], ECLI:EU:C:2003:596, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

European Court of Justice, Ruling C-362/14, *Schrems I*, 6th October 2015 ECLI:EU:C:2015:650 https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1039534

European Court of Justice, Ruling C-311/18, *Schrems II* on 9 May 2020, ECLI:EU:C:2020:559 https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

European Court of Justice, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, [2014] 1 C.M.L.R. 677. https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en

European Court of Justice, Ruling C-460/20 on 8 December 2022 Re V. Google ECLI:EU:C:2022:962 https://www.dpcuria.eu/case?reference=C-460/20

European Court of Human Rights, (2022), Case of M.D and others v. Spain. (Application no. 36584/17). https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-218034%22]}

European Commission. (2015). Communication From The Commission To The European Parliament And The Council on The Transfer Of Personal Data From The EU To The United States Of America Under Directive 95/46/EC Following The Judgment By The Court Of Justice In Case C-362/14 (Schrems). https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2015/0566/COM_COM(2015)0566_EN.pdf

Data Privacy Day. (2023). The most impactful ECJ judgments from the past years https://iabeurope.eu/cjeu-case-law-summaries/

Data Protection Officer, European Anti – Fraud Office (2016), Summaries of EU Court Decisions Relating To Data Protection 2000-2015.

http://traingrcy.law.uoa.gr/moodle/pluginfile.php/57/mod_resource/content/1/2%20caselaw_2001_2015_en.pdf