AMERICAN UNIVERSITY OF ARMENIA

ՀԱՅԱՍՏԱՆԻ ԱՄԵՐԻԿՅԱՆ ՀԱՄԱԼՍԱՐԱՆ

LL.M. Program

ԻՐԱՎԱԳԻՏՈՒԹՅԱՆ ՄԱԳԻՍՏՐՈՍԻ ԾՐԱԳԻՐ

TITLE

Comparative Analysis of privacy law between the United States and the EU. What will be the best practice for Armenia?

Whether GDPR as an evolution of Data Protection and United States regulations of Data Protection ensure the right of informational self-determination?

STUDENT'S NAME

Lusine Gevorgyan

SUPERVISOR'S NAME

PROF. Lilit Banduryan

NUMBER OF WORDS

8275

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia

Tel: (37410) 51 27 55
law@aua.am

Table of Contents

LIST OF ABBREVIATIONS 3

INTRODUCTION 4

CHAPTER 1 8

Self-Determination as a Fundamental Rationale Behind the Privacy Protection: Evolvement and Further Development

CHAPTER 2 12

Evolution of the Data Protection Law to Ensure Informational Self-Determination: The EU Right to be Forgotten in and the American Right to be Let Alone

CHAPTER 3 17

Illustration of the Right of Informational Self-Determination from the perspective of the Right of Data Portability

CHAPTER 4 23

Examination of the Law of the Republic of Armenia on Protection of Personal Data from the perspective of the right to Informational Self-Determination ……

CONCLUSION26

BIBLIOGRAPHY28

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia

Tel: (37410) 51 27 55
law@aua.am

LIST OF ABBREVIATIONS

GDPR	General Data Protection Regulation
USA	United States of America
WP29	Article 29 Working Party
DPD	Data Protection Directive
CoE	Council of Europe

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

"If we don't act now to safeguard our privacy, we could all become victims of identity theft".

-Bill Nilson

United States Senator

INTRODUCTION

At the beginning of the 20th century, the right to privacy and data protection emerged simultaneously in different parts of the globe, both within the common law and civil law systems. The right to privacy and data protection is considered to be a fundamental right which is enshrined in many international instruments. In accordance with Article 8 of the European Charter: *"Everyone has the right to the protection of personal data concerning him or her"*[1]. This right is not an absolute right and it can be restricted in exceptional circumstances. One of the first serious international discussions of data protection law took place in 1968 at the United Nations International Conference which led to the evolvement and development of a more rigorous protection mechanism not only under domestic legislation but also on the international level.

Years later the Committee of Ministers initiated a lengthy and thorough research and the outcome of the study triggered a compelling necessity to take legislative measures aimed at the protection of personal data. Thus, the development of data protection law in the European Union commenced in 1973 with the adoption of the first resolutions by the Council of Europe for the protection of individuals with respect to the processing of personal data. It was followed by the CoE Convention on the protection of individuals with regard to the automatic processing of personal data adopted in 1980. The right of personal data protection further evolved when in 1995 the European Community adopted the first data protection directive. The Directive regulated the issues relating to the processing of personal data kept in the databases of public institutions, such as ministries and hospitals. As a result of the rapid

[1] Charter of Fundamental Rights of the European Union (2000/C 364/01), Article 8

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

development of technologies and the availability of Internet across the world, the means and mechanisms of the use and processing of personal data become easier and people become more vulnerable in terms of protection of their personal data. As a stage of development, the right to privacy became a fundamental right.

In response to the new challenges of the ever-evolving world and as a result of new life situations and requirements of the current time which were not in any way regulated and addressed by the previous regulatory instruments, the European Union introduced the General Data Protection Regulation (hereinafter "GDPR") which has been adopted in 2016 and entered into force in May 2018. The main objective of the regulation is: *"the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data*"[2]. This objective of the regulation has been construed by some scholars in a quite unique manner. They indicate that: *"It is not the personal data as such that deserves protection, but the individuals to whom it pertains, and whose human dignity must not be endangered"*[3].

As for the United States, the protection of personal data is regulated both on the state and federal levels. In the course of the evolvement of the rights of data protection, only the Privacy Act of 1974 pertains to the protection of personal data in general. It governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in the systems of records by federal agencies. The remaining acts regulate the actions, rights, and obligations of information controllers of a specific sector, for instance, The Gramm Leach Bliley Act, which governs the standards of data protection obtained by banks, insurance companies or other financial institutions or The Health Information Portability and Accountability Act, which protects the information concerning health, but there is no other complete piece.

In the light of the provided historical background, it can be concluded that in the course of the 4th industrial revolution, the right of data protection which was recognized by the majority of countries at the beginning of the 20th century immensely evolved. Most of the countries either separately or in cooperation with each other take appropriate measures to ensure the protection of personal data without precluding the free flow of information and

[2] The EU general data protection regulation 2016/679 (GDPR), Article 1
[3] Radim Polcak and Dan Jerker B. Svantensson, Information Sovereignty, Data Privacy, Sovereign powers and the Rule of Law, 2017

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

without infringing the right to obtain information. These regulations undoubtedly contribute to the sustainable development of democratic societies. The right to Informational Self-Determination constitutes an inseparable part of privacy and personal data protection and the governmental authorities must make sure that the undertaken measures guarantee also the protection of that right in this digital era.

The concept of informational self-determination originated from German law. For the first time in 1983 the German Federal Constitutional Court recognized that every individual should have *"the authority to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others"* [4].

Despite the fact, that the existence and functionality of search engines make it practically impossible to exercise the right of informational self-determination, the regulations enshrined in GDPR essentially contribute to the full realization and materialization of the right of informational self-determination, which encompasses almost each and every right regulated and guaranteed by it. The protection by GDPR of the informational self-determination of data subjects will be illustrated via the analysis of the right to be forgotten which is a novelty embedded in GDPR and by the right to data portability.

The right to be forgotten derives from the case Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González, which had a tremendous impact on the inclusion of the right to be forgotten within the ambit of rights regulated by GDPR.

The elucidation of the notion of informational self-determination is more complex and intricate with regard to the respective acts of data protection of the United States. No explicit right to be forgotten exists in the legislation of the United States and the scholarly opinion with respect to the adoption of new acts conveying and regulating this right is not unanimous. Some scholars express legitimate concerns that the right to be forgotten is not in compliance with the constitution of the United States; particularly it contradicts the first amendment of the constitution which guarantees freedom of speech.

---

[4] Antoinette Ouvry and Yves Pullet, The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, 2009

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

This thesis paper shall consist of an introduction, 3 chapters, a conclusion, a bibliography. The **Introduction** will provide a general overview of the right to privacy and data protection and will emphasize Data Protection mechanisms and regulations implemented within the European Union and the United States. **Chapter 1** is designed to study the concept of informational self-determination, its origin, and further development, the scope of its application, as well as the number of rights guaranteed by the respective regulations that are included and are construed within the ambit of the concept. **Chapter 2** will study the extent of contribution of the GDPR and the regulations under corresponding acts of the United States to the full realization of the right of informational self-determination. It will further analyze the right to be forgotten and within the scope of informational self-determination. **Chapter 3** will focus on the analysis of the right to data portability from the perspective of Informational Self-Determination. **Chapter 4** offers insight on international best practices with regard to Informational Self-Determination and possible amendments required in the Armenian legislation on the matter, the **Conclusion** will succinctly outline the main findings of the research. Followed by a bibliography listing all the sources used for the paper.

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

CHAPTER 1

Self-Determination as a Fundamental Rationale Behind the Privacy Protection: Evolvement and Further Development

In 1968, one of the most prominent scholars of his time Alan F. Westin in his famous book "Privacy and Freedom" defined privacy as *"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."*[5] Back then he emphasized the importance of each individual to have absolute autonomy towards his personal data for the purpose of maintenance of privacy. Many years later a similar definition was used to describe the concept of Informational Self-Determination evolved within the scope of the right to privacy and data protection.

The notion of the basic right of informational self-determination emerged in Germany at the end of the 20th century and it was used and properly defined for the first time by the Federal Constitutional Court of Germany. In its decision with regards to the constitutionality of a Population Census Act adopted by the German federal parliament, the primary goal of which was the statistical census of the population, the court introduced a purely new and never before identified right, the so-called right of informational self-determination.

In 1983, after the adoption of the Population Census Act, a wave of resentment and rebellions started in different parts of Germany. Most of the population was against the conduct of the census by the government and the main grounds for their protests were the concerns that such a statistical census was an imminent threat of unlawful intrusion of privacy and the preclusion of enjoyment of private life by the citizens. The adoption of the Census Act had been characterized by the population as an obvious attempt to increase the surveillance and data processing by governmental authorities, as it contained a provision of

[5] Westin, A. 1967, 'Privacy and Freedom', Bodley Head, London. p. 7.

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

application and transmission of collected data [6]. The Census Act conveyed inquiries regarding the religion, the occupation, the place of work and education, etc. The extremist opponents even commenced a counter-movement raising issues of data protection which would result as a consequence of a population census, and ultimately the Census Act was challenged before the Federal Constitutional Court of Germany.

The same year the court rendered the decision that the aim of the census was justifiable, however, the court demanded to rectify the procedural and organizational mechanisms to guarantee the full protection of all the fundamental rights of people. Moreover, the data transfer to public authorities was declared unconstitutional. However, the case is considered to be a landmark case in the judicial system of German law not due to its outcome, but rather due to the identification of a new fundamental right.

The court perceived and defined the right to informational self-determination as *"the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others"*[7]. The right to informational self-determination is a quite unique right in its nature for it encompasses not only strong legal backgrounds but it also contains certain elements of sociology and even psychology. From the legal perspective, the Court based its reasoning on two fundamental rights guaranteed by the Constitution which are the protection of human dignity and the protection of general personal liberty of each individual and as a result of the combination of those two rights originated the right of personality.

An eminent German sociologist Niklas Luhmann describes the right of informational self-determination in the following manner: "*such rights …have the function of guarding the differentiation of society into sub-systems. The role of privacy, in particular, is to protect the consistency of the individuality of the individual, and consistent self-expressions rely heavily on the separation of societal sub-systems. Privacy and informational self-determination guard these separation lines, as they prevent sensitive information from one context (e.g. the working world, medical treatment, family life, etc.) from proliferating into other ones"*[8].

From sociological perspective personal data of each individual is inextricably linked with his personality and self-identification, therefore a person should have unrestricted

[6]Data protection in Germany I: The population census decision and the right to informational self-determination, Gerrit Hornung & Christoph Schnabel. University of Kassel, Germany
[7] See footnote 4
[8]See footnote 6

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

autonomy towards any data concerning his private life. The capacity of freely and independently determining the extent to which his personal data can be disseminated, as well as the manner in which that data is made accessible to the society, constitutes an inseparable part of human dignity. The unjust invasion of privacy and interferences with the private life of an individual disrupt the natural process of self-determination, and to some extent distort and sometimes even alter the personality of a particular individual. The ambiguity and vagueness with respect to the possibility of intervention with personal life, the fear of permanent surveillance and strict scrutiny by the governmental authorities and the anticipatory release of personal data to the public adversely affect the development of individualism and unique personality. Hence, the right to informational self-determination in line with the protection of personal data ensures free and self-determined development of each individual.

The right of informational self-determination including data protection is also a crucial element for the sustainable development of a democratic society. One of the cornerstones of democracy is the free and unconstraint expression of the will of the majority. The development of a society is fostered by the abundance of deliberative, independent and unrestricted citizens who participate in civil and public processes of their country seeking to improve the social and political life with the assurance that their public activity will not have any deterrent effect on their privacy. The decrease in the level of the protection of the right to informational self-determination may serve as a restraining mechanism compelling the individuals to be more careful and observant towards their actions and speeches as those public activates may result in the invasion of private life. Therefore, from the foregoing analysis of the right to informational self-determination from different standpoints, a plausible conclusion can be drawn that the promulgation and protection of this right contribute to a great extent to the natural growth of personality on the one hand and to the sustainable development of a democratic society on the other hand.

In comparison with German domestic legal order, the American legal system does not recognize the right to informational self-determination as such. An analogical right, mostly known as the "right to be left alone" appeared in American jurisprudence in the 1890s after the publication of an article by Warren and Brandeis in a Harvard Law Review, where the authors announced for the first time the existence of a "right to privacy". The protection of privacy is reflected by two kinds of privacy laws: sexual privacy and Fourth Amendment privacy.

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

Within the scope of sexual privacy and Fourth Amendment Privacy, the Supreme Court of the United States in some cases impeded the gathering of an individual's information by State Authorities basing its judgment on "respect for the inviolability of the human personality"[9]. In the case of *Boyd v. United States*, the Court even attributed special significance to personal security and personal liberty. In *Whalen v. Roe* case, which is considered to be a landmark case with respect to issues pertaining to privacy and data protection, the Court identified two interest to be addressed. The first one is "avoiding disclosure of personal matters" and the second one is the "independence of making certain choices"[10]. However, the Court did not develop sufficient case law to explicitly recognize and substantiate the existence of the right to informational self-determination in American jurisprudence.

In the course of recognition and penetration of the right to self-determination in the European law and the evolvement of its analogical right within the American legal system, the means and mechanisms of information collection and processing were not as sophisticated and easy as they are now. In the current era of globalization and the development of new technologies, the methods of personal data processing are becoming easier day by day. The existence, functionality and the percentage of accessibility of search engines by the vast majority of the world's population imposes a direct threat to the protection of the right to self-determination. Another layer of threat to the right of self-determination adds up almost universal usage of social networks where the personal data becomes available to the general public both voluntarily by data subjects and involuntarily which means that the personal data, sometimes even sensitive data is released to the public by third parties without the knowledge of data subject. These factors deprive data subjects from the autonomy with regard to their data and make the exercise of the right to self-determination almost infeasible.

In line with the development of means and methods of data processing, the legislative bodies of developed countries separately or in cooperation with each other elaborate and strengthen the regulatory mechanisms towards the processing of personal data which in their turn immensely contribute to the full realization of the right to self-determination by data subjects. In the following chapters, the extent of the above-mentioned contribution by the EU

[9] Murphy v. Waterfront Commissioner, 378 U.S. 52, 55 (1964)
[10] Whalen, 429 U.S. at 602-603

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

regulation and respective Acts of the US will be better illustrated by the analysis of separate rights which are within the ambit of the initial right to informational self-determination.

CHAPTER 2

Evolution of the Data Protection Law to Ensure Informational Self-Determination: The EU Right to be Forgotten in and the American Right to be Let Alone

When the right to privacy and data protection emerged at the beginning of the 20th century and consequently developed as a new and quite important branch of the law, in no legal instrument regulating the collection and processing of personal data an indication is made pertaining to the right of Informational Self-Determination. With the passage of time and under the pressure of the newly emerged requirements, the new legislative acts and regulations introduced new rights which ensured the realization of the right of Informational Self-Determination. In the European Union Directive on the protection of individuals with regard to the automatic processing of personal data and on the free movement of such data (hereinafter "Directive") adopted in 1995 which is the predecessor of GDPR the right to erasure of personal data has been introduced which was guaranteed to all data subjects.

General Data Protection Regulation adopted by the European Union in 2016 embedded in it a novelty, the right to be forgotten, to ensure the right of Informational Self-Determination. The right to erasure of personal data can, to some extent, be qualified as an implicit right to be forgotten, however, the first legal instrument that explicitly codifies, properly defines and regulates the right to be forgotten is GDPR.

Under Article 17 of GDPR: *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay in case the personal data are no longer necessary in relation to the purposes for which they were*

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

collected, the data subject withdraws consent on which the processing is based, the data subject objects to the processing, the personal data have been unlawfully processed, etc."[11].

It is obvious that the new General Data Protection Regulation has been elaborated for the substitution of the previous regulatory legal instrument which became obsolete and did not meet all the needs and requirements of contemporary life. The new regulation is developed to regulate newly emerged concepts, to address all the challenges in the era of technological innovations and eventually to set the all-encompassing criteria for the protection of privacy and personal data. Bearing in mind the prerequisites for the creation of GDPR, a legitimate question arises regarding the reasons and circumstances that triggered the explicit inclusion of the right to be forgotten within the scope of GDPR.

In 2014 prior to the adoption of GDPR, the Grand Chamber of the Court of Justice of the European Union adjudicated a case Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González pertaining to the protection of individuals with regard to the processing of personal data. On 5 March 2010, Mr. Costeja González, a Spanish national resident in Spain initiated proceedings against Google Spain and Google Inc. The applicant complained that when an internet user entered Mr. Costeja González's name in the search engine of the Google group he would obtain links to an announcement mentioning Mr. Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts [12]. He requested that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results as the information is currently irrelevant.

Based on the respective provisions of the CoE Directive which was the legal instrument in force at the time of rendering the judgment, the Court identified a specific right to be forgotten within the scope of the right to erasure of personal data. Moreover, in the judgment of the case concerning the erasure of personal data from the Google search engine the Court recognized the right of EU data subjects to request the removal of links by those search engines, who are also data controllers. Hence, the right to be forgotten derived from the above-mentioned case which is considered to be one of the reasons that had a tremendous impact on the inclusion of the right to be forgotten within the material scope of GDPR.

---

[11] The EU general data protection regulation 2016/679 (GDPR), Article 17

[12] Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, 13 May 2014, Judgment, para. 14

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

Despite the fact that the right has been construed and recognized by the Court of Justice of the European Union and it is explicitly mentioned in the General Data Protection Regulation, there are still challenges, the full realization of the right is not absolute and is subject to certain restrictions.

Recital 65 of the GDPR sets forth the grounds for the lawful retention of personal information of data subjects by the data controller[13].

- the right of freedom of expression and information,
- compliance with a legal obligation,
- the performance of a task carried out in the public interest,
- a task carried out in the exercise of official authority vested in the controller,
- public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
- the establishment, exercise or defense of legal claims

In accordance with Recital 73 of GDPR the right to be forgotten can be also restricted under such circumstances as public security, the context of criminal penalties and prosecutions, the protection of the freedoms of others[14]. Furthermore, GDPR, on the one hand, imposes an obligation on the controller to erase the personal data which it made public; on the other hand, it allocates a very wide margin of appreciation to the controller.

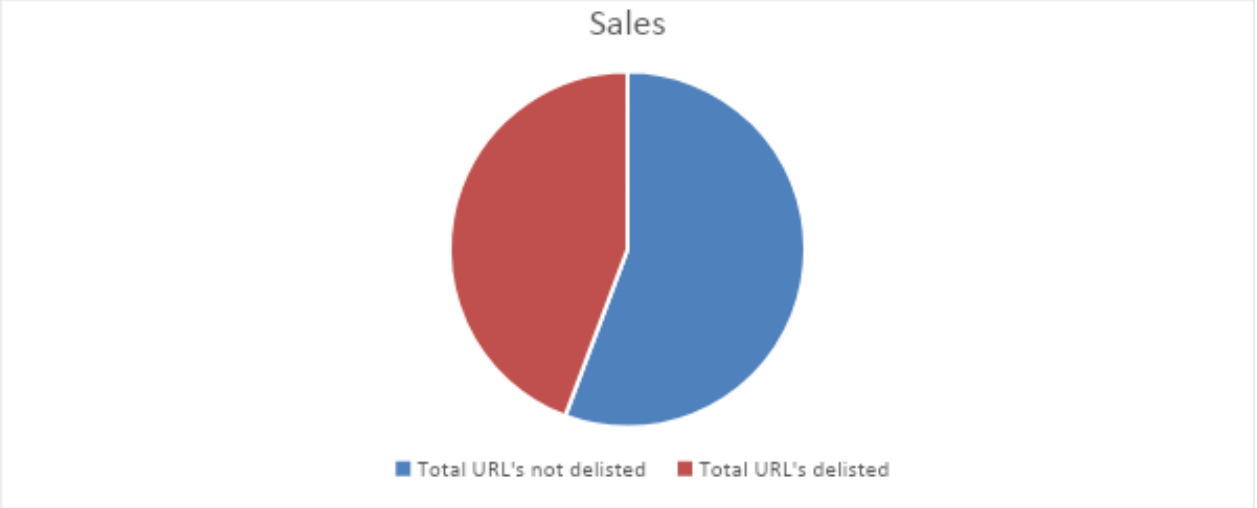
The complexity of the full realization of the right to be forgotten can be explained by the fact that though GDPR mainly pertains to the protection of personal data, it is also a unique example of a balancing mechanism between the right to privacy and data protection and the right to information. Thus while assuring the right to be forgotten to all data subjects, the GDPR also includes provisions that hold the equilibrium between the right to information. In the light of the presented exceptions from and restrictions on the right to be forgotten, as well as all the privileges granted to the controllers by the GDPR, it can be inferred that the pursuit towards the full realization of this right is not absolute, but at the same time feasible. For instance, the statistical data presented by Google Transparency Report according to which the company has delisted 44.3% of all URL removal requests, substantiates the foregoing

[13] Recital 65 EU GDPR
[14] Recital 73 EU GDPR

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

analysis that the realization of the right to be forgotten by data subjects granted and protected by GDPR is complex but feasible.

According to the Google's Transparency Report, the delisting takes place in the following manner: "We delist URLs from all of Google's European search results—results for users in France, Germany, Spain, etc.—and use geolocation signals to restrict access to the URL from the country of the requester". This statement illustrates that the realization of the right to be forgotten is possible; furthermore it is being exercised by many users each year.
The chart below shows the total number of requests received and the total number of URLs requested to be delisted since May 29, 2014[15].



In contrast to the European Law, no explicit right to be forgotten exists in the legislation of the United States and the scholarly opinion with respect to the adoption of new acts conveying and regulating this right is not unanimous. Some scholars even express legitimate concerns that the right to be forgotten is not in compliance with the constitution of the United States; particularly it contradicts the first amendment of the constitution which guarantees freedom of speech. The First Amendment to the US Constitution reads as follows: *"Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof, or abridging the freedom of speech or of the press, or the right of the people peaceably to assemble and to petition the government for a redress of grievances"*[16]. Those scholars also contend that the aim of the adoption of such acts is not the compelling

[15] Google's Transparency Report, Search Removals Under European Privacy Law
[16] The Bill of Rights, Amendment 1

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

need to protect the right of a data subject to request the erasure of information which undermines his dignity, but rather to acquire tools to restrain freedom of speech.

Thomas Jefferson with regard to the ten Amendments to the US Constitution, stated: *"A bill of rights is what the people are entitled to against every government on earth, general or particular, and what no just government should refuse, or rest on inference."* The historical development of each country is unique, consequently, the legal traditions formulated in the course of history and the perception of certain concepts vary from country to country. In 1791, when the Bill of rights was adopted, the population of the United States had gained its freedom from British Empire and the values they appreciated most of all were reflected in the ten Amendments to the Constitution. Those values crystalized by the course of the time and they are now deeply rooted in the national ideology of the United States.

While analyzing the evolvement of the right to be forgotten and its further codification in a legal instrument created by the European Union, it should be indicated that the necessity for the creation of such kind of right is a result of a natural development of a legal system which inevitably leads to the escalation of population's needs. On the contrary, the right to be forgotten has no legitimate place in the domestic legal order of the United States and even to some extent it is not in compliance with the core principles set forth and protected by the US Constitution.

Although an attempt is made by the State of New York with an "Act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act" to introduce the concept of the right to be forgotten into the American legal system, it has been highly criticized and the possibility that this act will ever become an integral part of American legislation is quite dubious. Therefore, the insertion of any legal norm into the legislative structure of a particular country should be analyzed in a broader context taking into consideration various factors, including legal traditions crystallized for many centuries, historical background and undoubtedly the anticipatory benefits of the norm on the population as a whole.

Thus, as opposed to the European legislation where the right to be forgotten is crystallizing and its realization becomes ever more feasible, the analogical right to be let alone is rather undermined. Though the balance between the right to be forgotten and the freedom of speech is a challenge for the European legislation as well, taken into consideration

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

the absolute nature of freedom of speech in the American legislation the scale leans here more towards the freedom of speech.

CHAPTER 3

Illustration of the Right of Informational Self-Determination from the perspective of the Right of Data Portability

The right to Informational Self-Determination is one of the main underlying principles of the General Data Protection Regulation and respectively, this right either explicitly or implicitly is reflected in almost each and every article included in the Regulation. However, in order to further illustrate the Right to Informational Self-Determination within the ambit of the European data protection regulation, this Chapter will focus on the thorough examination of another new yet fundamental right of data subjects embedded in General Data Protection Regulation known as the right to data portability.

Though the right to data portability is viewed by many scholars as a complementary to the right of access under the Data Protection Directive 95/46/EC, it is, in fact, a novelty as it differs in a number of substantive aspects from the right of access. As EU Justice Commissioner and Commission Vice-President Viviane Reding affirmed in a public statement, "17 years ago less than 1% of Europeans used the internet. Today, vast amounts of personal data are transferred and exchanged across continents and around the globe in

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

fractions of seconds"[17]. In fact, the necessity of inclusion of the right to data portability within the scope of GDPR arose as a result of new challenges triggered by the era of rapid technological developments and globalization, for instance the challenges that nowadays the internet users and particularly social media account holders face with regard to the protection and controllership over transmission of their personal data.

Another major difference between the right of access and the right of data portability which is a pure indication that the right to data portability is not a supplementary of the right of access but rather a newly emerged right is the format. In case of the right of access the data controller had absolute discretion in choosing the format to provide the requested information, whereas the right to data portability compels data controllers to provide the information in the machine-readable format which makes it more suitable for digital contexts and aims at empowering data subjects with respect to their own personal data by facilitating their ability to move, copy or transmit personal data easily from one IT environment to another[18]. In comparison with the right of access which is of general application, the right of data portability has a limited scope and is applicable only under certain circumstances and only with respect to the data initially provided by data subjects.

The right to data portability is contained under Article 20 of GDPR. It defines the right to data portability in the following manner: *"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided"*[19]. As it is elaborated in Recital 68 of GDPR, the purpose of incorporation of this right within the scope of GDPR is to further support user choice, user empowerment and to enhance the controllership of a data subject over his personal data.

The right to data portability is a two-fold right and the two main constituting elements are the right to receive personal data which fosters the controlling mechanisms of data subjects over their personal data and results to the solution of various issues arising mainly

[17] On the occasion of the press conference organized after publicly launching the content of the data protection reform in 2012
[18] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability, 16/EN WP 242 rev.01, 2017
[19] The EU general data protection regulation 2016/679 (GDPR), Article 20

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

with regard to digital platforms and service providers; and the right to transmit personal data from one data controller to another data controller which in its turn contributes to the interoperability between the services. For the purpose of a detailed analysis of the right to data portability of data subjects from the perspective of Informational Self-Determination, these two main elements comprising the right to data portability will be examined separately.

In accordance with the Guidelines on data portability of WP29 "the primary aim of data portability is enhancing individual's control over their personal data and making sure they play an active role in the data ecosystem."[20] This definition, to some extent, is an endorsement of the statement that the main objective and function of the first element of data portability is to guarantee that data subjects have a real opportunity to control, retrieve and re-use their data. Alternatively, a vast majority of scholars claim that the right to data portability may have an enormous impact with respect to resolving issues pertaining to the so-called lock-in effects in data-driven markets.

The lock-in effect of the users originates as a result of various factors taking place in the ever-evolving world of the market. Digital monopolies have incentives to protect their competitive advantage and to lock in consumers. Once users have made an investment in their current platform, the new platform has to duplicate that effort. In this sense, the degree of lock-in is determined by the level of switching costs. Users experience switching costs when they assess the investment required for changing to a new platform. This investment could be in a new equipment, in learning how to use a product, or even psychological.[21] In that case, providers could conceivably create switching costs, for instance by limiting the portability of customer data to and from competing services, in order to enhance customer lock-in[22].

The right to data portability helps to solve the issue of lock-in effect in a sense that data subjects will not be obliged to use an inferior product just because of high switching costs, as it grants them the opportunity to request from the controller the previously provided personal data in a structured, commonly used and machine-readable format which makes it

[20] See footnote 18
[21] Munich Intellectual Property Law Center (MIPLC), Enforcing data portability in the context of EU competition law and the GDPR, 2017
[22] Gabriela Zanfir, The right to Data portability in the context of the EU data protection reform, May 11, 2012

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

easier to transmit data from one controller to another controller without additional switching costs.

However, this approach is not unequivocal and it is still highly debated among experts and scholars. Some scholars contend that the contribution of the right to data portability towards the solution of such a major issue as the lock-in effect is insufficient. The main justifications for holding such a position are as follows:

1. The scope of the right of data portability is quite limited as it refers only to personal data previously obtained from the data subject based on his consent or as a performance of a contractual obligation and it explicitly excludes the data generated by the controller through the use of provided personal data.
2. Moreover, the wording of the regulation is confusing with respect to the type of data provided by data subjects; it does not specify whether it only refers to data provided by the data subject directly or also to data provided indirectly.

In response to the above-mentioned concerns, the Article 29 Working Party has presented a possible classification of personal data depending on the origin. This categorisation indicates the type of data that should be included as 'provided by the data subject':

- Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.)
- Observed data provided by the data subject by virtue of the use of the service or the device. They may, for example, include a person's search history, traffic data, and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.[23]

Irrespective of the mentioned limitations, the right to data portability may immensely contribute to the solution of the lock-in effect of data subjects. The provided clarification with respect to the term 'provided by the data subject' used in the context of the regulation indicates that the term should be interpreted broadly and it encompasses sufficient data to reduce the switching costs and not to constrain the data subjects while making a reasonable decision in favor of changing the service provider.

[23] Article 29 Working Party, 'Guidelines on the Right to Data Portability' (n 139) 10

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

Alternatively, the right to data portability may be seen as the valuable opportunity for an effective development of a user-centric platform where all digital services are interconnected. The capacity of a data subject to transmit information from one data controller to another data controller may, to some extent, encourage the usage of interoperable formats. In the market-driven world where all the companies and social networks irrespective of their size and provided services spend the huge chunk of their budget on creating new projects and mechanisms aimed at involving new customers and users should undoubtedly be interested in holding an interoperable format. One crucial element which may be an incentive to attract a great number of new users is the user-oriented approach of the company. In this regard, the capacity of a given company to accept the personal data of a potential user presented to it in a structured, commonly used, machine-readable format obtained by the user from the previous controller may serve as a perfect indication for future users and customers. A strong form of interoperability would enable consumers to transfer data seamlessly from one platform to another. Thus, the right to data portability not only encourages a real competition between service providers but it also avoids the monopolisation of the Internet by large companies.

Despite all the advantages and contribution of the right to data portability with respect to interoperability, the existence of major challenges impeding its full implementation is beyond a reasonable doubt. The main reason is the unclear and vague text of Article 20 of Data Protection Regulation which stipulates that the data should be provided in a structured, commonly used and machine-readable format, however, it does not specify what that format is, alternatively what standards should be used to determine the appropriate format. Recital 68 of the regulation adds another layer of ambiguity by stating that "Data controllers should be encouraged to develop interoperable formats that enable data portability" and further that this right "should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible".

Another challenge for the practical implementation of the right to data portability is the wording of the second part of Article 20 of GDPR which states that: *"the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible".* The inclusion of the phrase "where technically feasible" outrageously limits and precludes the exercise of the right to data portability, thus providing the controllers with real opportunity to abuse this clause and justify the rejection of data

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

transmission to other data controllers upon the request of data subjects as the format is not strictly identified by the regulation for the purpose of maintaining the market dominance.

However, the mere existence and inclusion of the right to data portability within the scope of such regulatory instrument as GDPR is a restraining mechanism and its elaboration via case law in terms of strict interpretation and clarification of the vague text of the regulation has a potential to eliminate all the obstacles precluding the full implementation of data portability regarding the interoperability between the service providers.

From the thorough examination of the background, purpose, and scope of the right to data portability it is easily detected that it perfectly illustrates the right of Informational Self-Determination.

CHAPTER 4

Examination of the Law of the Republic of Armenia on Protection of Personal Data from the perspective of the right to Informational Self-Determination

The aim of this chapter is, by thorough examination and illustration of the corresponding laws regulating the branch of law with regard to privacy and data protection, to reveal to what extent the right to Informational Self-Determination is included within the scope of the Armenian legislation and in case of necessity to make appropriate suggestions

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

based on international best practice and the comparative analysis of the European and American legislative acts governing the personal data protection.

In the Armenian legal system, the issues pertaining to privacy and personal data protection are regulated by the Law of the Republic of Armenia on Protection of Personal Data which has been adopted in June 2015. The main objective of the law is "*to regulate the procedure and conditions for processing personal data, exercising state control over them by state administration or local self-government bodies, state or community institutions or organizations, legal or natural persons*"[24]. The scope of the law is limited, it explicitly excludes the regulation of processing personal data exclusively for journalistic, literary and artistic purposes.

Taken into consideration the fact that Armenia belongs to the civil law countries and the perception of freedom of speech is not as acute as it is in the United States of America, it is definitely natural that the overall examination of the law indicates that the Armenian regulation of personal data protection has a certain resemblance with the European regulation rather than the American regulation.

Some aspects of resemblance are easily detected in the definitions of some crucial notions such as "personal data" and "processing of personal data". Below are presented extracts from GDPR and RA Law on Protection of Personal Data defining the indicated notions. The matching parts of the text are italicized.

General Data Protection Regulation

"personal data" *means any information relating to an identified or identifiable natural person;* an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person;

"processing" *means any operation or set of operations which is performed on personal data* or on sets of personal data, whether or not by automated means, such as *collection*, recording, organization, structuring, *storage*, adaptation or *alteration*, retrieval, consultation, use,

[24] Law of the Republic of Armenia on Protection of Personal Data, Article 1

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Law of the Republic of Armenia on Protection of Personal Data

"personal data" shall mean any information relating to a natural person, which allows or may allow for direct or indirect identification of a person's identity

"processing of personal data" *shall mean any operation or set of operations* irrespective of the form and mode of implementation thereof, which is related to the collection either stipulation or input or systematization or organization or *storage* or use or *alteration* or restoration or transfer or ratification or blocking or destruction of personal data or to carrying out other operations;

However, it cannot be stated that the RA Law on Protection of Personal Data is fully compatible with the requirements set forth by the General Data Protection Regulation. The RA Law on Protection of Personal Data has been adopted long before the European Data Protection Regulation entered into force and since then it has not been edited to be in compliance with the Regulation.

Irrespective of the fact that the Law of the Republic of Armenia on Protection of Personal Data has many substantial similarities with the European General Data Protection Regulation, the differences particularly in terms of the right of Informational Self-Determination are much more vivid. In contrast with GDPR where the right of Informational Self-Determination is explicitly illustrated in the vast majority of rights contained in the regulation among which are the right to be forgotten and the right to data portability, the Armenian law on Protection of Personal Data does not include any explicit provision which may indicate to the inclusion of the right of Informational Self-Determination within the material scope of the law. Neither the overall examination of the Law nor the detailed analysis of its Articles reveals any implicit reference to the right to Informational Self-Determination.

The analysis of the right to be forgotten and the right to data portability provided in Chapter 2 and Chapter 3 respectively, illustrate the utmost importance of the inclusion of the Right to Informational Self-Determination within the scope of the European comprehensive

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

regulatory mechanism and its immense contribution to the protection of personal data and to the strengthening of data subjects' control over their personal data.

Based on the fact that the protection of personal data is a relatively new brunch of law in the Republic of Armenia and the field is not highly regulated yet, the adaptation and practical implementation of European practice might be highly useful. Taking into consideration the results of the thorough examination of the Right of Informational Self-Determination and its illustration through separate rights and acknowledging the importance of this right with regards to personal data protection, this paper came to the conclusion that it is highly recommended for the purpose of strengthening the protection of personal data of data subjects to include the Right of Informational Self-Determination as one of the fundamental principles of RA Law of Personal Data Protection. It is also recommended to explicitly include articles granting data subjects with the right to be forgotten and the right to data portability.

CONCLUSION

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

The right to privacy and personal data protection emerged at the beginning of the 20th century and evolved ever since into a new and highly regulated brunch of law. The right to privacy and personal data protection is considered to be a fundamental right and it is guaranteed by various major international legal instruments. In the era of globalization and rapid development of technology, data subjects become more and more vulnerable and unprotected in terms of the controllership over their personal data which triggers a compelling necessity for the elaboration of sophisticated and comprehensive regulatory instruments.

In response to the new challenges of the rapidly developing world which jeopardize the protection of personal data and violate the fundamental rights of people, in 2016 the European Union introduced General Data Protection Regulation which entered into force in May 2018. The Regulation is a quite comprehensive document that encompasses a great number of rights addressing all the vulnerable aspects with regard to the processing of personal data of data subjects. Among numerous rights and principles, the Regulation also includes the right to Informational Self-Determination. This concept derives from German law and it was first used and properly defined by the Federal Constitutional Court of Germany.

The main rationale behind the right to Informational Self-Determination is the idea of the unequivocal authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others. Acknowledging the utmost importance of this right, the General Data Protection Regulation introduced new rights which ensured the full realization of the right of Informational Self-Determination.

One of those innovative rights ensuring the realization of the right of Informational Self-Determination introduced by GDPR is the right to be forgotten which is the right of data subject to obtain from the controller the erasure of personal data whenever the data are no longer necessary in relation to the purposes for which it has been collected. Irrespective of the existence of certain requirements precluding the full implementation and enjoyment of the right to be forgotten, the Google's Transparency Report indicates that each year more and more data subjects are successful in their pursuit of the implementation of this right.

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

Another right included within the scope of GDPR that illustrates the significance of the right to Informational Self-Determination is the right to data portability. The main objective of the right to data portability is to strengthen the controllership of data subjects and to empower them with respect to their own personal data by facilitating their ability to move, copy or transmit personal data easily from one IT environment to another. Despite all the ambiguity of the text and other challenges that may, to some extent, be impediments for the realization of this right to data portability, it has the full capacity to solve the issue of the users' lock-in effect with service providers.

Based on the examination of the right to Informational Self-Determination within the scope of General Data Protection Regulation and on the analysis of the accomplishments of the separate rights that ensure the realization of the right to Informational Self-Determination, it is highly recommended, for the purpose of further strengthening the data protection regulations in the Republic of Armenia, to include the principle of Informational Self-Determination and its derivative rights within the RA Law of Personal Data Protection.

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

BIBLIOGRAPHY

Charter of Fundamental Rights of the European Union (2000/C 364/01),
Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

The EU general data protection regulation 2016/679 (GDPR)
Available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

Radim Polcak and Dan Jerker B. Svantensson, Information Sovereignty, Data Privacy, Sovereign powers and the Rule of Law, 2017
Available at: https://www.cambridge.org/core/journals/international-journal-of-legal-information/article/information-sovereignty-data-privacy-sovereign-powers-and-the-rule-of-law-by-radim-polcak-and-dan-jerker-b-svantesson-northampton-ma-edward-elgar-2017

Antoinette Ouvry and Yves Pullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy" (2009),
Available at:
https://www.researchgate.net/publication/225248944_The_Right_to_Informational_Self Determination_and_the_Value_of_Self_Development_Reassessing_the_Importance_of_Privacy_for_Democracy

Westin, A. 1967, 'Privacy and Freedom', Bodley Head, London
Available at:
https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

Data protection in Germany I: The population census decision and the right to informational self-determination, Gerrit Hornung & Christoph Schnabel. University of Kassel, Germany

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

Available at:
https://www.unikassel.de/fb07/fileadmin/datas/fb07/5Institute/IWR/Hornung/Hornung___Schnabel__Data_protection_in_Germany_I__CLSR_2009__84.pdf

Murphy v. Waterfront Commissioner, 378 U.S. 52, 55 (1964)
Available at: https://supreme.justia.com/cases/federal/us/378/52/

Whalen, 429 U.S. at 602-603
Available at: https://supreme.justia.com/cases/federal/us/429/589/

The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 Am. J. Comp. L. 675 (1989)
Available at:
https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1865&context=facpubs

Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, 13 May 2014
Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Recital 65 EU GDPR
Available at: http://www.privacy-regulation.eu/en/recital-65-GDPR.htm

Recital 73 EU GDPR
Available at: http://www.privacy-regulation.eu/en/recital-73-GDPR.htm

Google's Transparency Report, Search Removals Under European Privacy Law
Available at: https://transparencyreport.google.com/eu-privacy/overview?hl=en

The Bill of Rights, Amendment 1
Available at:
https://nccs.net/blogs/americas-founding-documents/bill-of-rights-amendments-1-10

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

On the occasion of the press conference organized after publicly launching the content of the data protection reform in 2012.
Available at:
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=EN&guiLanguage=en. accessed 24 March 2012

ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the right to data portability, 16/EN WP 242 rev.01, 2017
Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Munich Intellectual Property Law Center (MIPLC), Enforcing data portability in the context of EU competition law and the GDPR, 2017
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203289

Gabriela Zanfir, The right to Data portability in the context of the EU data protection reform, May 11, 2012 Available at:https://www.academia.edu/3189962/The_Right_to_Data_Portability_in_the_Context_of_the_EU_Data_Protection_Reform

Law of the Republic of Armenia on Protection of Personal Data
Available at: http://www.foi.am/u_files/file/Personaldataprotectionlaw_ENG.pdf

Gabriela Zanfir-Fortuna, The Right to Data Portability in the Context of the EU Data Protection Reform, International Data Privacy Law, Vol. 2, No. 3, 2012
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2215684

Inge Graef, Martin Husovec, Nadezhda Purtova, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law, German Law Journal 2018, vol. 19 no. 6, p. 1359-1398
Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071875

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am

Peter Swire, & Yianni Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Md. L. Rev. 335 (2013)
Available at: http://digitalcommons.law.umaryland.edu/mlr/vol72/iss2/1

40 Marshal Baghramyan Avenue
0019, Yerevan, Armenia
Tel: (37410) 51 27 55
law@aua.am