www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
Volume I, No 4, December 2018
birci.journal@gmail.com, birci.journal.org@gmail.com
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

The Constitutional Context of Computing in Portugal - Article 35

Pedro Ramos Brandão
Évora University - Interdisciplinary Centre for History, Cultures and Societies

Abstract: *the creation and evolution of Article 35 of the Portuguese Republic's Constitution. The ordinary legislation related to article 35. European legislation related to the protection of personal data. The General Regulation of Data Protection.*
Keywords: *Portuguese Republic's Constitution; Article 35; general regulation on data protection; Judgement 182/89; Law 10/91; Law 41/2004; Law 67/98.*

I. Introduction

The Portuguese Republic's Constitution was conceived and written in a very specific intellectual environment, the end of an authoritarian dictatorship of the right deeply Catholic and castrating of fundamental rights, this historical fact is crucial to understand the conception of Portugal's main legal instrument after the military coup order of 25 April 1974.

For this reason, the original text is significantly innovative for its time, even in the context of comparative law. It is especially meticulous in the area of Fundamental Rights, Freedoms and Guarantees, and extraordinarily includes the issue of Computing in this area. With the introduction of the IT issue in the Fundamental Rights, Freedoms and Guarantees group, the Portuguese Constitution, at the time it was drafted, became one of the most innovative in Europe. Thus, Article 35 of the Constitution of the Portuguese Republic is dedicated to the consecration of fundamental rights in the area of the use of information technology, a truly innovative event for that time, in terms of Europe and the World. So, something unheard of at the time.

To a certain extent, the fact that the legislator has regulated the use of information technology within a restricted scope of rights, freedoms and guarantees is also innovative, thus subjecting itself to the specificity of the legal system expressed in Article 18 of the Portuguese Republic's Constitution, in which it has no special legal effect deriving from the rights covered, considering what its main characteristics are, namely, the direct application of constitutional precepts, the binding form of public and private entities, and proper reservation of the Law. However, Article 35 of the Portuguese Republic's Constitution is one of the most affected by changes over time. This is due in large measure to the fast-technological evolution that the area of computing and information technology suffers, and therefore requires adaptations resulting from these changes, whether conceptual or merely terminological.

This work is not a legal work, it is a work of history, developed through an objective methodology based on a contextualized chronological line and the content of legal and juridical instruments. It is studied the creation and evolution of Article 35 of the Portuguese Republic's Constitution and the ordinary legislation that in one way or another relates to the content of that primary document.

II. Review of Literature

2.1 Article 35 and Its Evolution

When the Constitution came into force [1], Article 35 consisted of three numbers. These three initial articles have the current correspondence to Articles 1, 3 and 5. The first number required the right of every citizen to know what was registered in the records, the right to know what the records were intended for, and the right to request changes and updates to those records. The second number dealt with the prohibition of specific data on political beliefs, religious faith or private life that could not be processed by computer, with the

exception of the objective being statistical purposes, but in which personal data were not identifiable. The third number was also a prohibition, in this case the allocation of a single national number. This prohibition stems directly from the framework we mentioned in the introduction, political police in the second half of the twentieth century had a centralized reference file of individuals from which to create profiles, for which all information about citizens was compiled into a register with a single number. This centralization of information with a single indexer allowed these police officers (where PIDE and STASI could be given as examples) to create a very detailed profile of citizens, including details of their personal lives and their intimacy. The prohibition foreseen in the initial number two of Article 35 was not immune to this problem. These prohibitions still remain in the Constitution today.

With Constitutional Law 1/1982, of September 30, the first revision of Article 35 was carried out. The expression "mechanical records" in number one is replaced by another expression, in this case "computer records", is an update of denomination considering the new terminologies in use, fully respecting the intention of the initial legislator. A new number two is added and the old one becomes number three, this new number two establishes the prohibition of access by third parties to files with personal data and their possible interconnection. In regarding to the new number three he is the old number two and the old number three passes to the new number five, but with a significant change. This significant change to the new number five, formerly number three, now includes a ban on computer processing of data concerning philosophical convictions and party or union membership of citizens. This revision introduces a new number, in this case number four, to specify how to define the concept of personal data for computer records issues, that definition by imposition of this number will be defined by law. This change produced a very unique case in terms of constitutional legislative tradition: "If Article 35 is found in the range of Personal Rights, Freedoms and Guaranties, it will be understood that the regime imposed by Article 18 of the PRC on the legal force of IRFs, that is, they are directly applicable precepts. Nonetheless, this new paragraph 4 in referring to the law the definition of personal data made paragraph 2 of the same constitutional article dependent on the intervention of the ordinary legislator for its enforceability "[2].

In this regard, the Constitutional Court decided to verify the unconstitutionality by omission of the legislative measure foreseen in number four of the thirty-fifth article of the Constitution, which according to that court was necessary to make the guarantee in number two of the same article feasible, Case 87-0298 and judgement No 89-182-P of 1 February 1989.

Judgement of the Constitutional Court nº 182/89 of 01-02-1989, Mário de Brito was the rapporteur:

"The grounds for the request have been summarized as follows: *1. The constitutional legislator, in its revision, added the new provisions of paragraphs 2 and 4 to the original text of Article 35 of the 1976 Constitution, while at the same time amending the wording of paragraphs 1 and 3 of the previous version; 2. It is precisely in the new provisions of those paragraphs 2 and 4 that they have imposed explicitly binding provisions: one in the sense of forecasting and disciplining by law exceptions to the rule prohibiting third party access to files containing personal data and their interconnection ; the other committing to the law the definition of the concept of personal data for computer recording purposes; 3. Despite its direct applicability, by virtue of Article 18 (1) of the Constitution, Article 35 is a norm that is unenforceable by its nature and structure, lacking "legislative legislative activity" in order to*

ensure its full applicability and practical operation; 4. This "fulfilling" activity - or interpositio legislatoris - is likewise implicitly claimed, in another perspective, for the normative purposes and the values, within the aforementioned constitutional precept, for whose pursuit it points, in its normative "unity" teleological; 5. Almost five years after the revision of the Constitution, "at the concrete and actual moment of history," truly positive acts "are not known, with a result" typified "in the Constitution or in the Assembly of the 'legislative omission' mentioned, that is to say, to comply with the constitutional levies established in paragraphs 2 and 4 of the aforementioned article 35. " (...) J. J. Gomes Canotilho and Vital Moreira wrote, ob. cit., no. II of the annotations to article 283, that there is the "legal duty imposed by the Constitution, whose non-compliance implies juridically constitutional omission", "when the Constitution: (a) establishes a concrete order to legislate; (b) it establishes a permanent and concrete imposition directed at the legislator (examples: creation of the National Health Service, creation of basic education, compulsory and free), (c) it establishes rules that, not being expressly configured as orders to legislate or constitutional impositions (eg law on the exercise of the right of opposition, law on crimes of political responsibility, etc.) '. In this case, it is requested that a breach of the Constitution be declared by omission of the legislative measures necessary to render its articles 35 (2) and (4) operative. This provision, subordinated to the heading "Use of information technology" and included in the chapter dealing with personal rights, freedoms and guarantees: 1 - All citizens shall have the right to have knowledge of what is recorded in computer records concerning them and of the purpose for which the information is intended, and may require the correction of data and its updating. 2. Third party access to files with personal data and their interconnection as well as cross-border data flows shall be prohibited except in exceptional cases provided for by law. 3 - Computing can not be used to process data relating to philosophical or political beliefs, party or trade union affiliation, religious belief or private life, except when processing non-individually identifiable statistical data. 4 - The law defines the concept of personal data for the purposes of computerized registration. 5 - The allocation of a single national number to citizens shall be prohibited. 3 - (...) In view of the foregoing, the Court of First Instance has decided: (a) to verify non-compliance with the Constitution by omission of the legislative measure provided for in Article 35 (4) thereof, (2) of that Article; b) Inform the Republic Assembly of this verification. " [3]

As far as the original number three is concerned, it goes on to number five, without alterations, and the text remains the same until today.

Constitutional Law No. 1/1989, of July 8, amended the main numbers of article 35 of the Portuguese Republic's Constitution and adds a new number, in this case number six. It is therefore a second constitutional revision. This revision brings the limit to number one, limiting the right of access to computer records in the case of state secrecy and secrecy of justice. There were no changes to numbers two and three. However, the scope of number four has been extended, including in this issue the definition of the concept of database and data bank, as well as the conditions of access, constitution and use of these by public and private entities. In this revision, a new paragraph 6 concerning the definition of the regime applicable to cross-border data flows is also introduced, establishing appropriate forms of protection of personal and other data.

Constitutional Law No. 1/1997, of September 20, made a last amendment of the constitutional text in Article 35. Number one now envisages a general authorization regarding the secrecy of the State and the secrecy of justice, with the purpose of the law being

able to restrict the right in cases of access to personal data entered in computerized records, in the cases mentioned.

Numbers two and four change their sequence and undergo minor changes. "*The alteration of order only gives greater sequential logic to the ordering of the precepts contained in the numbers resulting from successive revisions that did not always had this logical link at attention*." [2] Regarding the content of the numbers, now number two adds to the text the existence of an independent entity [4] that will be responsible for data protection guarantees, this entity is currently the National Data Protection Commission. [5]

With regard to number four, a general authorization for the legal restriction is added to exceptional cases legally established, the obligation to distinguish between database and data bank is also eliminated. Paragraph 3 now establishes a ban on the use of computing where there may be information about ethnic origin. The wording of number five remains the same.

The number six also suffers a change, guaranteeing free access to public computer networks by all citizens. This safeguard has a direct relation with Article 13 of the Portuguese Republic's Constitution, that is, with the question of equality.

In this constitutional amendment was added the number seven, extends to manual files has protection identical to computerized data. This amendment is justified by the extent to which the Constitution provides for the protection of personal data. [6]

2.2 The Ordinary Law and Article 35 of the Portuguese Republic's Constitution

Since the first revision of the Constitution that Article 35 imposes on the legislator the definition of personal data, however this only occurred in 1991, through Law 10/91, of April 27. Law 10/91 of 27 April harmonized the principles of Convention 108 of the Council of Europe on the issue of data protection and automated processing of data. [7]

Directive No 58 / EC of the European Parliament and of the Council of 12 July 2002 has been transposed into Portuguese law by Law No 41/2004 of 18 August. It refers to the processing of personal data and the protection of privacy in the electronic communications sector, repealing Law 69/1998, of October 28, becoming the national legislation for the issue of personal data processing in the electronic communications sector. Law 69/1998 does not explicitly define public data, so public data had to be understood as opposed to the definition of private data.

Law no. 67/98, of October 26, legally defines the concept of personal data. All definitions are laid down in Article 3 (a), (b), (c), (d), (f), (g), (h) and (i):

a) *'personal data' means any information of any nature whatsoever and independently of its medium including sound and image relating to an identified or identifiable natural person ('data subject'); a person who can be identified directly or indirectly, in particular by reference to an identification number or one or more specific elements of his or her physical, physiological, psychological, economic, cultural or social identity, shall be considered to be identifiable;*
b) *'processing of personal data' ('processing') means any operation or set of operations relating to personal data carried out with or without automated means such as collection, registration, organization, preservation, retrieval, consultation, use, communication by transmission, dissemination or any other form of making available, with comparison or interconnection, as well as blocking, erasure or destruction;*
c) *'personal data file' means a structured set of personal data, accessible according to specific criteria, whether centralized, decentralized or distributed in a functional or geographical manner;*
d) *'controller' means a natural or legal person, public authority, service or any other body which, individually or jointly with another person, determines the purposes and means of processing personal data; where the purposes and means of processing are determined by law*

or regulation, the controller shall be indicated in the law on organization and operation or in the statutory or statutory body competent to deal with the personal data concerned;

e) 'subcontractor' means the natural or legal person, public authority, service or any other body treating the personal data on behalf of the controller;

f) 'third party' means the natural or legal person, public authority, service or any other body which, other than the data subject, the controller, the processor or other person directly under the controller subcontractor, is empowered to handle the data;

g) 'recipient' means a natural or legal person, public authority, service or any other body to whom personal data are disclosed, whether or not it is a third party, without prejudice to the data are communicated within the framework of a legal provision

h) 'consent of the data subject' means any free, specific, and informed expression of will, under which the holder accepts that his or her personal data are processed;

i) 'data interconnection' means a form of processing consisting of the possibility of relating the data of a file with the data of a file or files held by another controller or others or held by the same controller for another purpose. [4]

This Law will also define how the treatment of sensitive data has to be done, through its article 7:

"The processing of personal data relating to philosophical or political beliefs, party or trade union membership, religious belief, private life and racial or ethnic origin, as well as the processing of data on health and sex life, including genetic data, shall be prohibited.

2 By means of a legal provision or authorization from the National Data Protection Commission, the data referred to in the preceding paragraph may be processed when, for reasons of important public interest, such processing is indispensable to the exercise of the legal or statutory attributions of its controller, or when the data subject has given their express consent to such treatment, in both cases with guarantees of non-discrimination and with the security measures provided for in Article 15.

3. The processing of the data referred to in paragraph 1 shall also be permitted where one of the following conditions is met:

a) be necessary to protect the vital interests of the data subject or another person and the data subject is physically or legally incapable of giving his or her consent;

b) be carried out, with the consent of the holder, by a non-profit-making foundation, association or non-profit-making body of a political, philosophical, religious or trade-union nature, within the scope of its legitimate activities, provided that treatment concerns only members of that body or persons with whom it maintains periodic contacts connected with its purposes, and that the data are not communicated to third parties without the consent of the owners;

c) it concerns data which are manifestly made public by the holder, provided that consent to the processing of those declarations can be legitimately deduced;

d) To be required for the declaration, exercise or defence of a right in judicial process and is carried out exclusively for that purpose.

4 - The processing of data on health and sex life, including genetic data, is permitted where it is necessary for the purposes of preventive medicine, medical diagnosis, medical care or treatment or management of health services, provided that the processing of such data is carried out by a health professional bound to secrecy or by another person also subject to professional secrecy, is notified to the National Data Protection Commission in accordance with Article 27 and that adequate information security measures are taken." [4]

Law n. 10/91, of April 29, as mentioned previously, through article 2, establishes that full name, affiliation, date of birth, parish of birth, identity card number and issuing contrary to these convictions in criminal proceedings, state of health, would have to be considered as personal data. [8] Law 67/98 of October 26, on the other hand, does not expressly state what public data are, so these will be understood as those that do not fit into the definition of private data. [4] This resulted in a clarification of this concept as paragraph 2 of Article 35 of the Portuguese Republic's Constitution.

Article 7, paragraph 1, of Law 67/98, of October 26, deals with the specificities of so-called sensitive or personal data, stipulating that this type of data is not subject to treatment:

"*1 - The processing of personal data relating to philosophical or political beliefs, party or trade union membership, religious beliefs, private life and racial or ethnic origin, as well as the processing of data relating to health and sex life, including genetic data, shall be prohibited. "* [4]

However, in the same article, but in paragraph 3, it makes an exception to paragraph 1 of that article:

3. The processing of the data referred to in paragraph 1 shall also be permitted where one of the following conditions is met:

To be necessary to protect the vital interests of the data subject or another person and the data subject is physically or legally incapable of giving his or her consent;

To be carried out, with the consent of the holder, by a non-profit-making foundation, association or non-profit-making body of a political, philosophical, religious or trade-union nature, within the scope of its legitimate activities, provided that treatment concerns only members of that body or persons with whom it maintains periodic contacts connected with its purposes, and that the data are not communicated to third parties without the consent of the owners;

To be related to data which are manifestly made public by the holder, provided that consent to the processing of those declarations can be legitimately deduced;

To be necessary for the declaration, exercise or defence of a right in judicial process and is carried out exclusively for that purpose.

Finally, in point 4 of Article 7 of Law No 67/98, the legislator is careful to specify separately the data concerning the health and sexual life of citizens, including genetic data, only necessary for the purposes of preventive medicine. [9]

This Law, in its article 5, deals with aspects related to how the data should be treated, it is even in 1998, a truly innovative aspect in terms of constitutional legal systems, in some other country of the Western world such specificity about personal data and its treatment is contained in the Constitutions. Article 5 incorporates five points:

a) *Treatable in a lawful manner and with respect for the principle of good faith;*
b) *Collected for specified, explicit and legitimate purposes and can not be further processed in a manner incompatible with those purposes;*
c) *Appropriate, relevant and not excessive in relation to the purposes for which they are collected and subsequently processed;*
d) *Accurate and, where necessary, updated, and appropriate measures shall be taken to ensure that inaccurate or incomplete data are erased or rectified, taking into account the purposes for which they were collected or for which they are subsequently processed;*
e) *Held in such a way as to enable the holders to be identified only for such time as is necessary for the purpose of collecting or further processing.*

Another innovative aspect of this law is the reference to "only for the period necessary for the pursuit of the purposes", that is to say, it limits the data storage in time, that in 1998, twenty years later, this rule will be included in the European proposal for the General Regulation on Data Protection (2018).

An important aspect is that of Law 67/98, to define very objectively what is the interconnection of data and to prohibit everything that is not legally foreseen, having to resort, in this case, to the National Data Protection Commission. According to this law the interconnection of personal data is: "form of processing consisting of the possibility of relating the data of a file with the data of a file or files held by another controller or others or held by the same controller for another purpose". [9]

As regards the rights of the data subject, Law 67/98 unfolds these rights in four separate rights, Articles 10, 11, 12 and 13. The right to information (Article 10), is the consecration of what is stated in Article 35 (1) of the Constitution of the Portuguese Republic *"right to know the purpose for which they are intended"*, the right of opposition can only be exercised if this right exists. The right of access (Article 11), the right to access data and to know them effectively and in full. The right of opposition (Article 12), here it is noted that the legislator sought to caution against prohibiting abuses in the use of personal data, is given the right to have the data updated and/ or rectified. The prohibition of automated individual decisions (Article 13), is a legislative interpretation of Article 35 of the Portuguese Republic's Constitution, deals with protection against risks of using information technology as a tool to limit fundamental principles.

This law also regulates the transfer of personal data outside the European Union (Articles 19 and 20). On the other hand, it creates and regulates the National Data Protection Commission (articles 21 and 32), highlights the three main attributions: 1st, control and audit compliance with legal and regulatory provisions on the protection of personal data; 2, to issue opinions on legal provisions; 3rd, authorize and record the processing of personal data.
Directive No 58 / CE / 2002 of the European Parliament of 12 July was transposed into the national legal system by Law No. 41/2004, of 18 August, this Law concerns the processing of personal data and the protection of the privacy in electronic communications. [10] [11]

Article 2 is complementary to Law 67/1998, in which the law will apply to the processing of personal data in the context of electronic communications networks and services accessible to the public, through Article 3, it broadens the application of "interests" subscribers who are legal persons to the extent that such protection is compatible with their nature. [11] In article 2, a more objective definition of some concepts that are totally emerging in contemporary society and usually used in imprecise contexts is defined, so the concepts of *"any connection established through a telephone service accessible to which allows real-time two-way communication* "[11]; subscriber*"a natural or legal person who is party to a contract with an undertaking providing publicly available electronic communications networks and / or services for the provision of such services*" [11]; electronic communication *"means any information exchanged or sent between a finite number of parties through the use of a publicly available electronic communications service, excluding information sent in connection with a service to the general public by means of a communications network which can not be related to the subscriber of an electronic communications service or to any identifiable user receiving the information* "[11]; location data "*any data processed in an electronic communications network indicating the geographical location of the terminal equipment of a subscriber or any user of a publicly available electronic communications*

service" [11]; user "*any natural person using a publicly available electronic communications service for private or commercial purposes, not necessarily subscribing to that service*" [11]; "*any data processed for the purpose of sending a communication through an electronic communications network or for the purpose of billing the same*" [11]; value added services "*means those who require the processing of traffic data or location data other than traffic data, in addition to the necessary transmission of a communication or the invoicing of a communication*"; [11] This legislative technique, which generated much disagreement and much controversy [2], however, is justified by technological developments and the extension of concepts and abstractions in the field of information technologies, may be useful if the law is extended to innovative scientific areas, whose concepts are not in law and jurisprudence [2].

This diploma also due to the new social and political context innovates in the field of the obligations of the service provider, which is a novelty. This is done through Article 3 of Law 41/2004. Faintly introducing the principles of self-regulation, which as it turned out do not work, so the future need for further regulation in this sector. This article establishes that there must be a principle of collaboration between companies providing electronic communications services, in order to guarantee the security of their services and of the network itself.

The guarantee of the confidentiality of communications, a subject of great public discussion, which becomes controversial with the public knowledge of what is done by the large state agencies of information and espionage, much due to information made public by people like WikiLeaks [12] and Edward Snowden [13], who has documented that the National Security Agency (NSA) systematically collects all the information circulating on the networks, and collects the data in a "gross" and "blind" manner, violating all laws of The United States of America as well as international laws. Similar news also becomes public in relation to Russia, China and North Korea, so the public is becoming aware of issues of mass breaches of confidentiality. Consequently, there is some pressure, even if it is in media, to legislate for the protection of confidentiality. In this sense, Article 4 of Law 41/2004 guarantees the confidentiality of communications and imposes on companies providing network and electronic communications services to maintain security systems that guarantee the inviolability of communications and their traffic data [11].

At a time when digital information is based on distributed computing and cloud computing, characterized by the fact that there is a geo-redundancy of all the information, which puts in question the possibility of a mathematically rigorous control of the information storage, because in distributed computing it is exceptionally difficult to control all information after it has been disseminated by all nodes or clusters. There is even an expression often used by technicians in the area of information technologies that is "... once on the Internet, forever on the Internet ..." which elucidates very well what happens to information in distributed computing systems. So, it is exceptionally difficult today to be able to track all the information stored on the Internet, and it is very difficult to know over time the physical location where this information is stored. For example, when you save a Microsoft Word file to a Cloud Computing system such as Microsoft's OneDrive just as you save the document, OneDrive automatically makes three copies of that document and delivers it to three Microsoft data centres scattered around the world, but if we pay to have a security redundancy called geo-redundancy, then every time a document is backed up to the Cloud Computing system, the same is replicated nine times and spread across multiple data centres.

In practice, we do not know where to store our document, and in case there is a failure of one of the data centres and the server cluster has to be partially removed it is possible that our document will be stored in the replaced set and the the exact notion of where all the auto copies of the documents are. So today, it is very difficult to ensure that the information owner knows exactly where their documents are, in case they use distributed computing systems or cloud computing systems. But Article 5 of Law No. 41/2004 imposes what in practice can be extremely difficult to achieve, or at least it will certainly be easy to violate this rule, which is only to allow the access or storage of information obtained through communications networks when two cumulative conditions are met: 1st - the prior information to the subscriber or user under the Data Protection Law; 2nd - the subscriber or user shall be entitled to refuse such processing. With regard to data storage specifically, it may be difficult to comply with this provision, you may already be easier on the access issue. It should also be noted that distributed computing systems can make automatic storage without information owners' knowledge, because this is the genesis of these systems and also because of the automation procedures for creating redundancy. On the other hand, it is important and even easier to implement the prohibition on the processing of location data, imposed by Article 7 of Law 41/2004.

III. Discussion

The General Regulation of Data Protection.

European history of data protection begins shortly after World War II with the creation of the Council of Europe, which brought together 10 European countries with the aim of promoting the rule of law, democracy and human rights. In 1950, the European Convention on Human Rights was adopted, which entered into force in 1953 in the legal system of all signatory countries. In 1959, with the creation of the European Court of Human Rights, it was ensured that all States fulfilled their obligations, and it was up to the Court to consider complaints submitted by natural or legal persons or by States or non-governmental organizations.

The right to the protection of personal data is one of the rights enshrined in the European Convention on Human Rights, in particular Article 8, which guarantees the right to respect for private and family life, home address and correspondence.

In 1981, as a consequence of the emergence in the 1960s of information technologies and the need for a set of resolutions on data protection, based on Article 8, in the following decade, Convention 108. This Convention applies to all processing of personal data by the public or private sector, including processing by police or judicial authorities, and is designed to protect citizens against abuses that may arise from the collection and processing of personal data. the cross-border flow of personal data. Also in Convention 108 are guarantees concerning sensitive personal data, such as race, political opinion, health, religious beliefs, sexual life or criminal record. Convention 108 was ratified by all Member States of the Council of Europe, and in 1999 it was amended to allow the European Union to join. It has 46 signatory States. As regards European Union law, its first legal instrument relating to data protection was Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data. which concerns the processing of personal data and the free movement of such data.

Regulation 45/2001 laid down rules for the protection of natural persons with regard to the processing of personal data by Community institutions and bodies, since the 1995

Directive referred only to Member States and not to the European Union itself. In 2000, the European Union proclaimed the Charter of Fundamental Rights of the European Union. This was subsequently made legally binding in the Treaty of Lisbon in 2009 as a primary right of the European Union. Article 7 of the Treaty of Lisbon laid down the principle of respect for private and family life and Article 8 of the Treaty on the right to data protection.

The Federal Regulation of Data Protection is only the culmination of all these intentions materialized and not materialized in the above-mentioned instruments. The General Data Protection Regulation is a European regulation, endorsed by the European Parliament and the European Council, which regards the protection of natural persons with regard to the processing of their personal data as a fundamental right regardless of their nationality or place of residence. to achieve an area of freedom, security and justice and an economic and social union in Europe. The Regulation seeks to harmonize and safeguard the fundamental rights and freedoms of natural persons, but also to ensure the free movement of personal data between the Member States of the European Union. A European regulation, unlike a directive, is of direct application in the legal system of the different States of the European Union, without having to be transposed into national law. It has a threefold objective: to harmonize legislation, consistency in the processing of personal data throughout the European area and legal certainty [14].

The need for the European Union to legislate on personal data protection has resulted from a number of factors, such as the increase in cross-border flows and, as a consequence, increasing economic integration as a result of the creation of the single market as well as the result a growing exchange of data between the public and private sectors, continuous technological change.

IV. Conclusion

The Constitution of the Portuguese Republic through its article 35 was universally innovative, compared with other Constitutions, regarding the consecration of fundamental rights related to information technology and protection of personal data. It has been evolutionarily updated to keep up with changes in society and technology. When European laws emerge on this matter, it turns out that the essence that justified this legislative production has long been a concern mirrored in the Portuguese Republic's Constitution.

References

[1] CRP, "Portuguese Republic's Constitution - Approval Decree No. 0/1976, dated 04/10/76".

[2] P. Venâncio, "Constitution: the use of computing," Revista de Estudos Politécnicos (Journal of Polytechnic Studies), 2007.

[3] Agreement no 182/89. Diário da República no. 51/1989, Series I of 1989-03-02, 1989.

[4] Law no. 67/98 of October 26, 1998.

[5] General Regulation of Data Protection.

[6] Article 35 of the Portuguese Republic's Constitution, 1997.

[7] Convention 108 of the Council of Europe (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), adopted in Strasbourg on 28 January 1981, 1981.

[8] Law No. 10/91, 1991, 29 April.

[9] Law no. 67/98 of October 26, 1998.

[10] Directive No 58 / EC / 2002 - European Parliament, 2002.

[11] Law No. 41/2004, 2004, 18 August.
[12] Wikileaks, "Wikileaks," [Online]. Available: https://wikileaks.org.
[13] Snowden, "Snowden," [Online]. Available: https://twitter.com/snowden.
[14] N. Saldanha, New General Regulations on Data Protection, Lisbon: Lidel, 2018.