

**DANILO DONEDA<sup>1</sup>**

**MARIO VIOLA DE AZEVEDO CUNHA<sup>2</sup>**

**Data protection as a trade resource in Mercosur:  
a data protection framework as an integrative tool.**

---

<sup>1</sup> PhD in Private Law (Rio de Janeiro State University), Professor of Private Law at Campos Law School (Rio de Janeiro, Brazil) and specialist in data protection in Latin American countries.

<sup>2</sup> LLM in Private Law (Rio de Janeiro State University - Brazil), Master of Research (European University Institute - Italy), PhD Candidate (European University Institute - Italy) working in the field of data protection in Europe and Latin America and one of the coordinators of the CEULAS Working Group (Law Department of the European University Institute), a Multidisciplinary Working Group on Comparative European and Latin American Studies.

## **Table of contents:**

**1. Introduction: the importance of information and the necessity to protect privacy**

**2. The international nature of data protection**

**3. The European Model of Data Protection as an integrative tool**

3.1. Limits for the collection and use of personal data

3.2. The storage and transfer of personal data

3.3. Institutional and regulatory bodies

**4. Data protection in Mercosur**

4.1. Argentinean System

4.2. Uruguayan System

4.3. Paraguayan System

4.4. Brazilian System

**5. Conclusions**

## 1. Introduction – The importance of information and the necessity to protect privacy

From a historical perspective, the need to protect privacy started to be discussed only at the end of the 19th century, in the famous article “The right to privacy”, written by Louis Brandeis and Samuel Warren,<sup>3</sup> which dealt with the protection of privacy, but only in relation to some aspects which did not include data protection. This aspect came into picture only in the 20th century, during the 60’s.<sup>4</sup> It is important to notice that the collection of personal data for credit purposes started during the first half of the 19th century, having as a reference the activity developed by the British Bank “Baring Brothers”.<sup>5</sup> With the increase in trade, many credit information agencies were created, culminating with the development of huge consumer information databases, with the aim of facilitating credit.

Although, as said above, governments’ concern over the protection of personal data emerged in the 60’s and the first international instruments to deal with data protection were developed only at the beginning of the 80’s. An important example of this can be seen in the Council of Europe Convention n° 108 of 21.01.1981, for the protection of individuals with regard to the automatic processing of personal data, that in its preamble states that *“it is desirable to extend the safeguards for everyone’s rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing”*.<sup>6</sup>

However, the recent advances of technology have undoubtedly broadened and sophisticated the treatment and the flow of personal data, facilitating and increasing trade all over the world. Despite of the positive aspects of such advances, they can violate freedoms and

---

<sup>3</sup> DONEDA, Danilo. “Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade”, in: TEPEDINO, Gustavo (org.) Problemas de direito civil-constitucional. Rio de Janeiro: Renovar, 2000, pp. 111-136.

<sup>4</sup> See the case ‘National Data Center’. In DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, P. 184/190.

<sup>5</sup> EFING, Antônio Carlos. Bancos de Dados e Cadastros de Consumidores. São Paulo: Revista dos Tribunais, 2002. P. 22/23.

<sup>6</sup> Available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>. (25.01.08)

fundamental rights, in particular the right to privacy, which brings the necessity to create instruments that guarantee, at the same time, the protection of the individual concerning the use of his personal data, and the reasonable confidence for the economic institutions that use personal data for the development of their activities. In fact, during the last years the protection of personal data has been developed from these two perspectives.

The creation of economic blocks, such as Mercosur, intensifies crossborder flow of personal data as a consequence of the increase of trade between the Member States, making necessary the establishment of an uniform trade ambient which guarantees the protection of personal data within the block, avoiding different levels of protection among Member States, which could create barriers to the free movement of goods and services that use this kind of information. In this sense, the establishment of a minimum level of data protection inside Mercosur in economic activities that use personal data for the development of their business would facilitate the usage and the exchange of personal data among its Members States and also between Mercosur and other countries or economic blocks, favoring an appropriate ambient for industries that use personal data for the development of their activities.

A good example that could serve as a parameter for Mercosur, is the European initiative of harmonization of data protection rules among its Member States, which efforts are represented by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and the work that has been developed by Article 29 Working Party, aiming at facilitating the flow of personal data among its Member States, allowing the free movement of services that use this kind of data, such as the financial ones, and strengthening its integration process.

Nevertheless, the adoption of norms concerning data protection in Mercosur would imply, besides a mandatory legislative process, specific changes on the behavior of private and public sectors, which would have to observe additional procedures when treating personal information. This change, that includes, for example, the training of specialized staff in the field of data protection and the adequacy of internal and external procedures, would have a direct impact on the final costs of their activities. On the other hand, the adoption of such procedures would allow those entities to access a larger number of markets, as well as to improve their image due to their lawful processing of personal data and their endorsement of a policy that

respects individual rights.

Taking into account this scenario and considering personal data protection as an integrative tool, this paper will analyze the different systems of data protection of Mercosur Member States, pointing out their differences and similarities, and, then, suggest solutions, legislatives or not, aiming at harmonizing data protection within the block and, thus, assisting the development of the integration process of Mercosur. A wide range of solutions will be considered in our analysis: (1) the private and contractual option, with the adoption of specific contractual clauses; (2) the contractual option that uses standard clauses; (3) deontological norms and codes of practices; (4) public regulation in the format of a general law of data protection or fragmented rules; and, finally, (5) the establishment of a national authority to guarantee the effectiveness of the data protection system.

## **2. The international nature of data protection**

Personal information has an increasingly important role in international commerce as the gathering and treatment of such information becomes easier and more useful due to the recent progress of technology. Even though this is a fact with implications in various fields, it happens that its international dimension is something more than just the global scale projection of some country-specific situations. Instead, it is rather indispensable to define the very nature and scope of data protection, even when dealing with issues of a merely national or regional interest.

Recent legislative developments related to data protection usually stress two main points: the fact that protect personal data is one necessary step to protect people themselves in a time when a substantial part of our data (and our lives) is in digital form; and that the coherence between the set of rules regarding data protection in different countries is crucial for a lawful flow of information - and of commercial relations - between these countries to be possible and efficient.

Therefore, it soon became clear that a data protection framework would be of interest not only to the countries that felt the need to protect their citizens from the effects of abusive use of their personal information, but also to regional blocks of countries that,

besides their citizens' interests, would be eager to make their laws regarding data protection compatible and even interchangeable, in order to keep deals involving the international transfer of personal data as noise-free as possible, whenever that deal does not interfere with their citizens' rights.

Indeed, regional efforts to build these regional frameworks are anything but new. The European experience is already consolidated since its first Directive in 1995<sup>7</sup> and its roots can be traced at least as far as the time of the Convention n. 108 of the Council of Europe, 1981,<sup>8</sup> as mentioned before. Lately, some efforts have been seen from APEC (*Asia-Pacific Economic Cooperation*) to give their Member States a common approach to privacy and data protection by issuing in 2005 the *APEC Privacy Framework*.<sup>9</sup> Mercosur is yet in a very early stage in dealing with data protection, although the discussion about this issue has already begin - it should be emphasized that one of Mercosur's Member States, Argentina, has its own data protection framework which, by the way, complies with European Union's standards (as recognized by European Commission).

The international dimension of data protection has to be taken into account whether when looking at it in a global perspective or in a single country's framework. Its nature is the main reason for this - the technology that permits a widespread use and transmission of information almost regardless of physical barriers is the very reason of the problem to deal with data protection solely in national terms. Technology, thus, is the main element to define this situation, as in earlier stages of the privacy protection there was no big worry about international transfer of data in a time when databases were not digitalized and there were no easy way to transfer cheaply and flawlessly great amounts of data.

The picture today is different: technology cleared much of the issues that forbade personal data to be globally reached and used and the duty of establish rules for

---

<sup>7</sup> KUNER, Christopher. *European Data Protection Law and Online Business*. Oxford University Press: New York, 2003. P. 17.

<sup>8</sup> KUNER, Christopher. *European Data Protection Law and Online Business*. cit., Preface – P. ix.

<sup>9</sup> More information on the Framework and Principles is available at: <<[http://www.apec.org/content/apec/publications/free\\_downloads/2005.html](http://www.apec.org/content/apec/publications/free_downloads/2005.html)> and <[http://www.apec.org/content/apec/apec\\_groups/committees/committee\\_on\\_trade/electronic\\_commerce.html](http://www.apec.org/content/apec/apec_groups/committees/committee_on_trade/electronic_commerce.html)> (21/09/08).

the transmission and use of personal data has gone to the law itself, acting as a regulator of a process made possible just recently. Given the state of art, it is all but unnatural that the companies and entities that make use of personal data prefer to do this in an ambient as free as possible of law's constrains in order to obtain the maximum usefulness possible of this data. So the tendency - and the "attraction" - of personal data to be treated in countries with a weak legal framework on data protection - sometimes true "no-law" zones that permit operations with personal data that would be prohibited in the country of living of the people who are the true subjects of this data. The need to think globally in information-related issues dates, in fact, from the time of a historical international treaty was developed in another field with a strong dependence of its international effects, that is intellectual property and the Berne Convention of 1896, a historical example of legislative harmonization in a field in which this is a true necessity.

The need to follow the global reach of commercial relations guides the development of law in the field of data protection. It is relevant that one of the earliest international documents that approached the internationalization of data protection took into account the need to harmonize rules in order not to compromise international commercial relations, as it was the case of the OECD Guidelines of 1980.<sup>10</sup>

Some authors argue that, as does Colin Bennett, data protection laws face an inclination to convergence<sup>11</sup>, as could be seen by the adoption of similar sets of rules in different countries, as well as by the reduced role that national particularism usually plays. Indeed, one of the questions to be answered in the following decades is if data protection will be able to be independent of national regulation and if this is a desirable goal.<sup>12</sup>

At the present, there is no global rule or treaty regarding data protection in a consistent way. In the lack of formal global regulation, it is worth mentioning that when establishing legislation related to data protection issues, the most prominent legal instruments seems to be the mentioned OECD's *Guidelines on the Protection of Privacy*

---

<sup>10</sup> Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, available at: <[http://webdomino1.oecd.org/horizontal/oecdacts.nsf/linkto/C\(80\)58](http://webdomino1.oecd.org/horizontal/oecdacts.nsf/linkto/C(80)58)>. (05.03.08).

<sup>11</sup> See Colin Bennett, *Regulating privacy, Data protection and public policy in Europe and the United States*, Ithaca: Cornell University Press, 1992, pp. 116-152.

<sup>12</sup> Natalino Irti. *Norma e luoghi. Problemi di geo-diritto*. Bari: Laterza, 2001, p. 11.

*and Transborder Flows of Personal Data* of 1980, the *EU Data Protection Directive* of 1995, and the *APEC Privacy Framework* of 2005.

The very emergence of global data protection rules have been object of discussion for as far as its global impact has been recognized. As far as we are of recognizing the viability of such a rule, it is worth mentioning that - and maybe not only for practical reasons, some argue that European Union's standards are in the course of becoming a *de facto* global norm. Some evidence of this move can be gathered from a survey by the International Monetary Fund that noted that 29 out of the 31 countries whose economy is qualified by IMF as "advanced" have privacy legislation that is broadly similar to European Union standards - the only exceptions being United States and Singapore. The idea of European Union's standards being prominent is also supported by the idea that the international harmonization in this field tends to be done among higher degrees of protection rather than lower ones.<sup>13</sup>

So, as the global context plays a decisive role on the efficacy of any national standard to be adopted, it can be established that data protection law tend to harmonize first in a regional level and then going to the next, international level. The regional experience can demonstrate some of what was already said, in terms that the very existence of data protection laws in a country can affect directly the neighbor countries - as in a hypothetical case when neighbor countries with strong commercial ties don't share equivalent standards of data protection, causing the treatment of personal data to be preferably done in the country with the less restrict rules and, thus, submitting citizens of both countries whose personal data is involved to the less protective law.

---

<sup>13</sup> "As the process of globalization of our culture continues, there will be increasing pressure towards harmonization of international law relating to publicity and personality rights. (...) From experience derived from the harmonization of European laws on copyright and related rights, the probability is that harmonization will tend to select high degrees of protection rather than low ones. Two factors determine this outcome. First, European Union law respects vested rights of individuals: any harmonization which results in individuals in any European Union State receiving a lesser degree of protection than they enjoyed before harmonization is therefore out of the question. Secondly, on pure pragmatic grounds, equality of protection between contracting States can be effected as soon as legislation is implemented, without any need for a transitional period, if the maximum term of protection is selected. If, however, the minimum level of protection is selected, a significant transition period would be required before equalization was achieved in all contracting States". Michael Henry. *International privacy, publicity & personality laws*. London: Butterworths, 2001, p. 5.

It is not an easy task to analyze the different approaches to data protection between different countries, but some general conclusions can be empirically made: the countries that present the most developed laws about data protection are mostly developed and industrialize countries, whereas those with weak or no legislation at all are mostly developing countries.<sup>14</sup> The reasons for this concentration are many but the fact is that data protection legal reasoning came later to these countries, as is the case of all of Mercosur Member States.<sup>15</sup>

The regional impact of data protection laws can be summarized in two main situations: (i) the mere fact of the close political, social and commercial relations due to neighborhood can cause one country's law about data protection to have a direct impact on another's; (ii) a political move towards commercial integration in a certain region should, sooner or later, approach the issue of harmonization of data protection rules within these countries, in order to avoid extra costs and social damages.

Mercosur, a Regional Trade Agreement between Argentina, Brazil, Paraguay and Uruguay, is a typical case of regional integration that can profit from a common data protection framework, both in economic as in integrative terms, as can be perceived from European Union's example. As in Europe, it can be a tool for economic integration, that would be perceived both from the inside (eliminating barriers caused by the incompatibility of data protection laws) as from the outside (making it possible to Mercosul members to access foreign markets that have their own laws establishing a certain level of protection to personal information).

Apart the economic argument, it must be remembered also that the very essence of data protection is its goal to protect people's privacy in Information Society and this point shall be taken in to account when prospecting a Mercosur framework on data protection. It has been said several times that data protection is one of those rights with two different but indispensable goals: protect people's privacy and create an appropriate ambient for international commerce. The tension between this two goals is often used to

---

<sup>14</sup> As can be observed in the global map of data protection laws made by David Banisar in 2007 (in a Privacy International survey): <<http://www.privacyinternational.org/survey/dpmap.jpg>>.

<sup>15</sup> The first data protection law was enacted, indeed, in a country where the Welfare State reached a very sophisticated level of planning and implementation, thus creating the need for an instrument for the protection of citizens' private data. This law was the Swedish *Datalag* of 1967.

promote data protection sometimes as a commercial resource and others as a fundamental right that must be considered<sup>16</sup> and is one of the main factors behind the tendency of tying together data protection and international commerce and to push for international rules, as once noted Joel Reidenberg: "A new international data privacy treaty will be essential for the long-term, robust growth of e-commerce".<sup>17</sup>

### **3. The European Model of Data Protection as an integrative tool**

The European model, as said before, is a clear example of how data protection can act as an important factor in the integration process, specially concerning the establishment of a single market. Since it has as its main purposes "(1) to allow for the free flow of data within Europe, in order to prevent the Member States from blocking inter-EU data flows on data protection grounds, and (2) to achieve a harmonized minimum level of data protection throughout Europe"<sup>18</sup> it can be used as a source of inspiration for other economic blocks, such as Mercosur.

This free flow of information among the Member States of the block plays an important role in the creation of a single market, since "*Information has become the new raw material of the world economy. Just as, in past centuries, iron, wood, and coal were the foundation upon which the economy was based, so nowadays it is data and information.*"<sup>19</sup>

In this article we will analyze the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which is the general rule about data protection in the European Union and that has as objectives, on one hand, to guarantee the protection of individuals' privacy and, on the other, to allow the free flow of data among the EU Member States, strengthening the internal market.<sup>20</sup> In this sense is

---

<sup>16</sup> The mentioned tension is most visible in the European Union legislation to be further analyzed.

<sup>17</sup> Joel Reidenberg. "E-commerce and transatlantic privacy", in: 38 *Houston Law Review* 717 (2001), p. 749.

<sup>18</sup> KUNER, Christopher. *European Data Protection Law and Online Business*. Oxford University Press: New York, 2003. P. 17.

<sup>19</sup> KUNER, Christopher. *European Data Protection Law and Online Business*. Cit., Preface – P. ix.

<sup>20</sup> "*The legal basis of the General Directive was Article 100<sup>a</sup> of the Treaty of Rome (currently Article 95 of the Amsterdam Treaty), which provides for the adoption of 'measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have their object the establishment and functioning of the internal market' and mandates 'a high level of protection' in*

## Article 1(1)(2) of Directive:

### Article 1

#### Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.<sup>21</sup>

This flow of information among the member states of an economic block is of vital importance for the free movement of services, specially the financial ones, since their business depend on the collection of personal data. The existence of different levels of data protection, as the ones that can be found in Mercosur, increases the costs for the movement of services among its Member States, since companies will have to adequate themselves to different models of protection. The establishment of a common level of data protection, as the one implemented by the European Union through Directive 95/46/EC, could reduce such differences and facilitate cross-border services.

The above mentioned Directive is divided into three basic pillars: a) data protection itself, with the establishment of limits for collection and use of personal data; b) the control over storage, transfer and flow of data; and c) the creation of a regulatory and institutional structure to monitor the application within the EU Member States of the provisions of the Directive 95/46/EC. We will dedicate one topic for each one of the pillars.

### 3.1. Limits for the collection and use of personal data

In its first part Directive 95/46/EC deals with the limits for the collection and use of personal data. Some of the most important issues concerning such use are those related to the consent of the data subject.

---

*matters concerning consumer protection (...)*” In KUNER, Christopher. European Data Protection Law and Online Business. Cit., P. 29.

<sup>21</sup> “*This means that Member States cannot impose legal restrictions on data transfers or data flows to another Member State based on the level of data protection in such other Member State.*” In KUNER, Christopher. European Data Protection Law and Online Business. Oxford University Press: New York, 2003. P. 29. It is important to notice that all Member States of the European Union have to observe the provisions of the Directive 95/45/EC what guarantees a standard level of personal data protection and allows free data transfers or data flows among Member States.

The Nuremberg Code,<sup>22</sup> published in 1947, presented, as a way to alert society about the atrocities committed during the Second World War, “the voluntary consent of the person who will be submitted to a research”<sup>23</sup> as an essential step. In the same direction were the first legislations to regulate data protection, which placed consent as an important element to legitimise the collection of personal data.<sup>24</sup>

So, in the hypothesis that a company, such as an insurer, intends to send information about a consumer to a joint database of the insurance market, for example, concerning a subscribed insurance policy or a loss, this insurer will have, according to the Directive 95/46/EC, to obtain explicit authorization from the insured party, which can be made through a contractual clause, observing the provisions of articles 4 and 5 of the Directive 93/13/EEC on unfair terms on consumer contracts.<sup>25</sup>

Although consent on its own is not enough to authorize the collection and use of

---

<sup>22</sup> Article 1. The voluntary consent of the human subject is absolutely essential. This means that the person involved should have legal capacity to give consent; should be so situated as to be able to exercise free power of choice, without the intervention of any element of force, fraud, deceit, duress, over-reaching, or other ulterior form of constraint or coercion; and should have sufficient knowledge and comprehension of the elements of the subject matter involved, as to enable him to make an understanding and enlightened decision. This latter element requires that, before the acceptance of an affirmative decision by the experimental subject, there should be made known to him the nature, duration, and purpose of the experiment; the method and means by which it is to be conducted; all inconveniences and hazards reasonably to be expected; and the effects upon his health or person, which may possibly come from his participation in the experiment. The duty and responsibility for ascertaining the quality of the consent rests upon each individual who initiates, directs or engages in the experiment. It is a personal duty and responsibility which may not be delegated to another with impunity. Available at <http://www.hhs.gov/ohrp/references/nurcode.htm> . (05.03.08).

<sup>23</sup> DALLARI, Dalmo de Abreu. Ética Sanitária. Available at <http://www.saudepublica.bvs.br/itd/legis/curso/html/a09.htm> (11.03.07). Non-official translation of the author.

<sup>24</sup> In this sense is article 7 of the French Act n° 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties. Available at [http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17\\_definitive.pdf](http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive.pdf). (09.04.08). “Article 7 - Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l’une des conditions suivantes (...)”

<sup>25</sup> Article 4. 1. Without prejudice to Article 7, the unfairness of a contractual term shall be assessed, taking into account the nature of the goods or services for which the contract was concluded and by referring, at the time of conclusion of the contract, to all the circumstances attending the conclusion of the contract and to all the other terms of the contract or of another contract on which it is dependent. 2. Assessment of the unfair nature of the terms shall relate neither to the definition of the main subject matter of the contract nor to the adequacy of the price and remuneration, on the one hand, as against the services or goods supplied in exchange, on the other, in so far as these terms are in plain intelligible language.

Article 5. In the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favourable to the consumer shall prevail. This rule on interpretation shall not apply in the context of the procedures laid down in Article 7 (2).

personal data, it is essential that the data subject is able to give free<sup>26</sup> and informed<sup>27</sup> consent. In this sense Article 7 (a) of the Directive 95/46/EC establishes that “Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent.”<sup>28</sup>

This means that the data subject has to have an exact understanding of why his personal data will be collected and the destination that will be given to it, and thus be able to consciously express his consent.<sup>29</sup> On consumer credit contracts, for example, which are typical mass contracts, if the consumer refuses to give the information asked for by the bank, he will not be able to conclude this contract.

It is true that consent is necessary and has to exist but it is only the first step, and must be followed by other steps, to authorize the collection and the use of specific personal information.<sup>30/31</sup> The other steps to legitimise the collection and use of personal data, according

---

<sup>26</sup> Article 29 Working Party on Data Protection. Working Document on the processing of personal data relating to health in electronic health records (HER). Adopted on 15 February 2007. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp131\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf). P. 8. “Consent must be given freely: ‘Free’ consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as ‘free’. Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a *fait accompli* cannot be considered to be valid.”

<sup>27</sup> Article 29 Working Party on Data Protection. Working Document on the processing of personal data relating to health in electronic health records (HER). Adopted on 15 February 2007. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp131\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf). P. 9. “Consent must be informed: ‘Informed’ consent means consent by the data subject based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, in particular those specified in Articles 10 and 11 of the Directive, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject. This includes also an awareness of the consequences of not consenting to the processing in question.”

<sup>28</sup> The Article 29 Working Party created four criteria to verify if the consent is valid. “(...) consent must be a clear and unambiguous indication of wishes; consent must be freely given; consent must be specific; consent must be informed.” In KUNER, Christopher. *European Data Protection Law - Corporate Compliance and Regulation*. 2.ed. Oxford: Oxford University Press, 2007. P. 67.

<sup>29</sup> Article 2(h) of the Directive 95/46/EC establishes that “the data subject’s consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.”

<sup>30</sup> The Directive 95/46/EC brings some exceptions concerning the obligation to obtain the consent of the data subject. One of them is the case where the data is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. CAREY, Peter. *Data Protection: A Practical Guide to UK and EU Law*. P. 7.

<sup>31</sup> DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. P. 373-378.

to the Directive 95/46/EC, are the principles of finality (or purpose)<sup>32</sup> and of proportionality and the duty to inform of data collector.<sup>33</sup> The first one functions as a limit for consent, excluding the idea of generality. According to this principle, consent has to be given for one or more specific purposes.<sup>34</sup> So, the generic consent for any use of the data cannot be accepted.<sup>35</sup>

It is important to notice that the data collected has to be relevant and compatible with the purposes of the collection, and not excessive.<sup>36/37</sup> In this sense, a company cannot, let us use again the example of the insurer, for health insurance purposes, ask the insured party information

---

<sup>32</sup> Article 29 Working Party on Data Protection. Working Document on the processing of personal data relating to health in electronic health records (HER). Adopted on 15 February 2007. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp131\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf). P. 6. “Use limitation principle (purpose principle): This principle partially embodied in Article 6(1)(b) of the Directive, among others, prohibits further processing which is incompatible with the purpose(s) of the collection.”

<sup>33</sup> There are other data protection principles in the Directive that are recognized by the doctrine, but some of them are included in the ones that we mentioned (legitimacy and transparency) and the others are not relevant for the limits of use and collection of personal data, which is the focus of this topic. See KUNER, Christopher. European Data Protection Law and Online Business. Oxford University Press: New York, 2003. P. 17/18. “The content of the General Directive is often expressed in terms of six main principles which underlie it:

*Legitimacy: personal data may only be processed for limited purposes;*

*Finality: personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes;*

*Transparency: the data subject must be given information regarding data processing relating to him;*

*Proportionality: personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed;*

*Confidentiality and security: technical and organizational measures to ensure confidentiality and security must be taken with regard to the processing of personal data; and*

*Control: supervision of processing by DPAs must be ensured.”*

<sup>34</sup> Article 29 Working Party on Data Protection. Working Document on Genetic Data. Adopted on 17 March 2004. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2004/wp91\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_en.pdf). (10.05.08). P. 6. “The respect of the finality and proportionality principles imply a clear determination of the purpose for which genetic data are collected and further processed. To avoid incompatible re-use it is essential that the purposes for processing genetic data are clearly defined.”

<sup>35</sup> DONEDA, Danilo. Da privacidade à proteção de dados pessoais. P. 383.

<sup>36</sup> Article 29 Working Party on Data Protection. Working Document on the processing of personal data relating to health in electronic health records (HER). Adopted on 15 February 2007. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp131\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf). P.9. “The data quality principle: This principle in the Directive requires personal data to be relevant and not excessive for the purposes for which they are collected. Thus, any irrelevant data must not be collected and if it has been collected it must be discarded (Article 6(1)(c)). It also requires data to be accurate and kept up-to date.”

<sup>37</sup> Article 29 Working Party on Data Protection. Working document on biometrics. Adopted on 1 August 2003. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp80\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf). P. 6. “According to Article 6 of Directive 95/46/EC, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. In addition, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed (purpose principle). (...) Furthermore, an evaluation of the respect for proportionality and the respect for legitimacy is necessary, taking into account the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way.”

about his car or computer, and, for car insurance, it cannot ask information about the insured party's health.

Article 6 (1) (a)(b) of Directive 95/46/EC establishes that the purposes for the collection of personal data shall be specified in detail until the moment of its collection, which means that the use of the data is predetermined. In this case, the data collector has the duty of identifying all potential uses of the collected data and ensures that the data subject will be adequately informed.<sup>38</sup> The data collector also has the duty to inform the data subject about who will have access to such data and if it can be transferred to third parties. Thus, if a company obtains personal data for a specific purpose, such as the conclusion of a contract, this company must not make this information available to other companies of the same economic group. This situation would only be allowed if the data subject had authorized the data transfer.<sup>39</sup>

Besides, the kind of data that can be transmitted to third parties must be related to the object of the contract concluded between the data subject and the data collector, and has to be linked to the new destination of such data, for example a new contract.<sup>40</sup> Therefore, as discussed before, consent on its own cannot be the only element to legitimise the collection and use of personal data. This collection and use have to observe the finality and proportionality principles and the data collector has to accomplish its duty to inform the data subject. This is what can be extracted from Articles 6(1)(b)(c) and 7 of the Directive 95/46/EC.<sup>41</sup> Moreover, personal data must be processed in a fair and lawful way, according to Articles 5 and 6(1)(a) of the Directive

---

<sup>38</sup> CAREY. Peter. *Data Protection: A Practical Guide to UK and EU Law*. P. 54.

<sup>39</sup> DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. P. 339.

<sup>40</sup> CAREY. Peter. *Data Protection: A Practical Guide to UK and EU Law*. 2.ed. New York: Oxford University Press, 2004. P. 54.

<sup>41</sup> Article 6. 1. Member States shall provide that personal data must be: (...) (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

Article 7. Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

95/46/EC.<sup>42</sup>

So, the limits on legitimizing the collection and use of personal data are the principles of finality and proportionality, and must be preceded by the accomplishment by the data collector of its duty to inform the data subject about the purposes of the collection, the destination of the data, if that data will be transferred to third parties and any other details that can guarantee the free and informed consent of the data subject and the observation of the finality and proportionality principles.

### 3.2. The storage and transfer of personal data

The second part of the Directive 95/46/EC regulates the storage, transfer and flow of information, and this has a good reason, “*Gradually the world economy is transforming itself from an industrial-based economy to an information-based economy, in which the free exchange of information has become the life-blood of modern business life.*”<sup>43</sup> Let us start with an important source of information for the financial market that is the access to existing databases (e.g. credit databases).<sup>44</sup> Both banks and insurance companies would, as a first step, consult

---

<sup>42</sup> Article 5. Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

Article 6. 1. Member States shall provide that personal data must be: (a) processed fairly and lawfully. About the fairness of the processing of personal data see WEBSTER, Mandy. *Data Protection in the Financial Services Industry*. Gower Publishing Limited: Aldershot, 2006. P. 22/23. O autor apresenta os critérios criados pelo ‘Information Commissioner’ do Reino Unido para avaliar se um processamento de dados é lícito e leal. “*Some of the questions the Information Commissioner will ask when assessing fairness are:*

*Was the person supplying the data under the impression that it would be kept confidential by the data controller and was that the impression justified by the circumstances?*

*Was any unfair pressure used to obtain the information? Were any unjustified threats or inducements made or offered?*

*Was the person improperly led to believe that they must supply the information, or that failure to provide it must be disadvantage them?*

*(...) Personal data must be processed in accordance with any relevant legal requirements, both civil and criminal.”*

<sup>43</sup> NUGTER, A.C.M. *Transborder Flow of Personal Data within the EC: A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and The Netherlands and their impact on the private sector*. Kluwer Law and Taxation Publishers: Deventer, 1990. P. 1.

<sup>44</sup> In the United States, for example, the insurance industry has a joint database called MID (*Medical Information Bureau*) that collects information about the health status of the insurance applicants. ALLEN, Bill; MOSELEY, Ray. *Privacy and Health Insurance: Can Oil and Water Mix?* In ALMEDER, Robert F.; HUMBER, James M. (editores). *Privacy and Health Care (Biomedical Ethics Reviews)*. Humana Press: Totowa, 2001. P. 135. “*The MID is an insurance-industry clearinghouse that collects information on*

internal and external databases (consumer credit databases, for example) to confirm the authenticity of the data informed by the potential client and to obtain other information that might be important for the accurate risk analysis. However, the data subject will be protected by the provisions of in article 12 of the Directive 95/46/EC.<sup>45</sup>

Although, the maintenance of such databases involves the respect of certain rights in favour of the data subject. The first of the rights of the data subject concerning the collection and storage of his personal data is the right to be communicated by the controller “in an intelligible form of the data undergoing processing and of any available information to their source” (article 12(a), 2<sup>nd</sup> paragraph). It is important to notice that, in spite of the fact that no provision in the Directive exists concerning the moment when the communication has to be made, there is a unanimous view that the data subject must be communicated before information is entered into the database.<sup>46</sup>

Another important right of the data subjects concerning the storage of their personal data on databases is the right that gives them the possibility to gain access to their information

---

*insurance applicants submitted by member insurance companies and releases that data to other insurance companies who may be considering the applicant's request for new or increased coverage. The MIB contends that its files do not contain raw medical data, but merely codes noting that some member insurers has declined or restricted coverage based on categories of medical data it ascertained. MID policy states that other member insurers are not allowed to make underwriting decisions based on the information from the MID. Rather, the information merely serves as a red flag alerting the insurer considering the application that the applicant has sought coverage before and the category of the data, which may lead the insurer considering coverage to conduct their own investigation or request for information form the applicant's medical record. It is impossible to verify whether this is how the information is actually used.”*

<sup>45</sup> Article 12. Right of access. Member States shall guarantee every data subject the right to obtain from the controller: (a) without constraint at reasonable intervals and without excessive delay or expense:  
- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,  
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,  
- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);  
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;  
(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

<sup>46</sup> Article 29 Working Party on Data Protection. Working Document on Blacklists. Adopted on 3 October 2002. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2002/wp65\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp65_en.pdf). (09.05.08). P. 8. “One way of avoiding errors and problems would be to lay down a reasonable period between notification of the data subject and the actual entering of the information on the joint file, and this procedure could also apply to files on breaches of monetary obligations” (footnote n° 8).

and to check if information related to them is being processed, the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed (article 12(a) 1<sup>st</sup> paragraph). After gaining access to such information, the data subjects will have the possibility to rectify, erase or block the processing of data if there is any inaccuracy (article 12(b) and article 6(1)(d)).<sup>47</sup>

In this sense, a consumer, at any moment, will have the right to request the controller of the database access to his personal data stored, and, in the case that he finds an error, he can request rectification, erasure or the blocking of the respective data. If the administrator of the database refuses to give access or to rectify, erase or block the personal data, the data subject will be able to use not only administrative measures through national supervisory authorities (article 28)<sup>48</sup> but also through judicial remedies regulated by national rules of the Member States

---

<sup>47</sup> Article 6 (1)(d) establishes that “1. Member States shall provide that personal data must be: (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified”.

<sup>48</sup> Article 28. Supervisory authority. 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them. 2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. 3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim. Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place. 5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public. 6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State. The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information. 7. Member States shall provide that the members and staff of the supervisory authority,

(article 22).<sup>49</sup>

Another important issue is related to the period during which personal data can be stored. Article 6(1)(e) of the Directive 95/46/EC establishes:

Article 6

1. Member States shall provide that personal data must be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

However, there is no provision in Directive 95/46/EC nor is there any unanimous view on how long this period should be, since information stored in a file or database must be accurate and up to date (article 6(1)(d)): *“this entry may not be maintained once a debt has been paid off, even when overdue, while in others the information may stay on record for a maximum period which varies from one country to another. Notwithstanding these divergences, what is clear is that the principle of updating information entails an obligation clearly to reflect the fact that the debt has been paid off even if the entry on non-payment is maintained beyond the date of full repayment.”*<sup>50</sup>

In the words of A.C.M Nugter *“it should make no difference to either multinational companies or data subjects whether data processing operations take place in one country or in one or more others countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests.”*<sup>51</sup> Those are the main objectives of Directive 95/46/EC: allow the free flow of data within the EU without forgetting to guarantee the right to privacy of the individuals.

---

even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

<sup>49</sup> Article 22. Remedies. Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

<sup>50</sup> Article 29 Working Party on Data Protection. Working Document on Blacklists. Adopted on 3 October 2002. Available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2002/wp65\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp65_en.pdf). (09.05.08). P. 5.

<sup>51</sup> NUGTER, A.C.M. Transborder Flow of Personal Data within the EC: A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and The Netherlands and their impact on the private sector. Kluwer Law and Taxation Publishers: Deventer, 1990. P. 4.

### 3.3. Institutional and regulatory bodies

The last part of Directive 95/46/EC, but not less important, establishes a regulatory structure to be created by the Member States with the aim at controlling the accomplishment of the provisions of the Directive and also of national rules that incorporated such provisions. Article 28(1)(2) establishes that:

#### Article 28

##### Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

To accomplish such responsibilities, these authorities have investigative powers, effective powers of intervention and powers to engage in legal proceedings.<sup>52</sup> And all these powers have a justification, they are responsible for monitoring the application of the Directive's rules in their Member States, playing an important role in the development of a single internal market and a free area of data transfer and data flow, since "the existence of divergent national provisions leads to additional costs, administrative and organizational problems, or may even lead, though in practice only occasionally, to a total prohibition" of data flow or data transfer among the involved countries and, of course, "creates uncertainty for those who are dependent

---

<sup>52</sup> See Article 28(3): "3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts."

on the free flow of personal data”, such as the financial services.<sup>53</sup>

Besides this supervisory structure, the Directive creates, in its Article 29, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (known as Article 29 Working Party), that is an independent and advisory body, composed by the representatives of the Data Protection Authorities of all Member States, that has attributions to: (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures; (b) give the Commission an opinion on the level of protection in the Community and in third countries; (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms; (d) give an opinion on codes of conduct drawn up at Community level.<sup>54</sup>

Considering the fact that the Working Party is composed by representatives of all Member States who work in the field of data protection, it is possible to say that it has a privileged view of the situation of all Member States concerning the issues that arise from the use, transfer, and flow of personal data, and can identify if there are differences among the laws or practices of Member States and propose solutions.<sup>55</sup>

Finally, taking into account the system created by Directive 95/46/EC, it is possible to say that the European Model of data protection acts as an integrative tool, in the sense that it allows the free flow of personal information among its Member States, creating an ambient for

---

<sup>53</sup> NUGTER, A.C.M. Transborder Flow of Personal Data within the EC: A comparative analysis of the privacy statutes of the Federal Republic of Germany, France, the United Kingdom and The Netherlands and their impact on the private sector. Cit., 1990. P. 320.

<sup>54</sup> Article 30 - 1. The Working Party shall:

- (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;
- (b) give the Commission an opinion on the level of protection in the Community and in third countries;
- (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;
- (d) give an opinion on codes of conduct drawn up at Community level.

<sup>55</sup> Article 30 (2)(3)(4): “2. *If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.*

3. *The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.*

4. *The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.”*

the free movement of services, at least financial services.

#### **4. Data protection in Mercosur**

Mercosul, the Regional Trade Agreement among Argentina, Brazil, Paraguay and Uruguay, as of yet doesn't have any regulation regarding data protection, however, such issue has been discussed internally, as mentioned above.

The regulation of data protection in the region is done by means of national legislation and, in this issue Mercosur's Member States present a discrete discrepancy regarding their own data protection laws. In short, it can be said that Argentina has a general law strongly based in European standards, Uruguay has a brand new law with concrete ties also to European roots while Brazil presents some general constitutional provisions together with somewhat strong sectorial data protection regulation but no general data protection law, and, finally, Paraguay has constitutional provisions as well as a data protection law. It is worth elaborating the internal provisions of these countries.

Data protection, not only inside Mercosur but in Latin America as a whole, is a more recent issue than in Europe or U.S. The earlier specific mentions of issues regarding personal data are generally linked to the need to rebuild the events related to dictatorship, particularly the fate of disappeared people - and with this aim in mind it was set up the writ of *habeas data*, the right to access. *Habeas data* is a tool for access and correct personal data typical of some Latin America's countries legal systems. The writ, first introduced by the Brazilian constitution of 1988, has a consistent influence in many Latin American's countries, and in all of Mercosur's Member States.

##### **4.1. Argentinean System**

Out of Mercosur's Member States, it is Argentina the one with the richest experience in data protection. The fact that a data protection general law exists since 1999 plays a major role, and the consistent scholar and jurisprudential attitude towards

data protection adds to the fact that it is in Argentina that the major judicial and cultural penetration of data protection issues can be found in Mercosur and probably the whole Latin America.<sup>56</sup>

The basis of Argentina's framework is its constitutional provision for the protection of intimate life (article 19 of the Constitution)<sup>57</sup> and the right to intimacy as stated in article 1071 of the Civil Code.<sup>58</sup>

In 1994 it was introduced in Argentine's constitution a specific provision about personal data that became known as the *habeas data*, located in the third part of its article 43.<sup>59</sup> It is worth mention that even before the *habeas data* was said to be part of Argentine's legal system, as some regional provinces have their own law about this subject.<sup>60</sup>

---

<sup>56</sup> Even before the Argentine data protection law was enacted, some commentators stressed the strength of the Argentine's Constitutional provisions regarding data protection. Clèmerson Clève, "*Habeas data*: algumas notas de leitura", in: WAMBIER Teresa Arruda Alvim (coord.). São Paulo: RT, 1998, pp. 74-82, p. 81.

<sup>57</sup> Art. 19. "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

Section 19. - The private actions of men which in no way offend public order or morality, nor injure a third party, are only reserved to God and are exempted from the authority of judges. No inhabitant of the Nation shall be obliged to perform what the law does not demand nor deprived of what it does not prohibit. (English traduction available in <[http://www.argentina.gov.ar/argentina/portal/documentos/constitucion\\_ingles.pdf](http://www.argentina.gov.ar/argentina/portal/documentos/constitucion_ingles.pdf)>.

<sup>58</sup> "Art. 1071bis. El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y en hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá este, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación". For an explanation of the Courts' approach to this rules, see: Alejandra Gils Carbó. *El derecho a la intimidad y a la autodeterminación informativa*. Buenos Aires: La Ley, 2001, pp. 21-25.

<sup>59</sup> Art. 43, 3º parágrafo: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística".

"Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired. When the right damaged, limited, modified, or threatened affects" (English traduction available in <[http://www.argentina.gov.ar/argentina/portal/documentos/constitucion\\_ingles.pdf](http://www.argentina.gov.ar/argentina/portal/documentos/constitucion_ingles.pdf)>.

<sup>60</sup> Pablo Palazzi; Roberto Chacon de Albuquerque. "Habeas data e protección de datos personales en el Mercosur", *mimeo*.

The Argentine *habeas data* is a writ based on the *amparo*.<sup>61</sup> It establishes a right to access personal data in the hands of third parties, as well as a right to rectify, update or, if possible, delete the information. The usefulness of the provision made various provinces enact their own data protection laws based on the Constitution, causing the *habeas data* to assume a number of roles related to data protection.<sup>62</sup> Afterwards, a national data protection law was enacted in 2000 (Law 25326, October 4th, 2000) regulating *habeas data*, although it that can be also considered a general data protection law. Its model is based on the Spanish data protection law and, thus, follows in general terms the European standards.<sup>63</sup> In fact, after having some points of its effectiveness cleared with *Decreto Reglamentar* n°. 1558/2001, Argentina applied for the recognition of its data protection framework as being adequate according to the procedures described in article 29 of Directive 46/95/CE and was successful, being the first Latin American country which data protection framework is considered by the European Commission as country that complies with EU's standards, benefiting from the commercial advantages of this situation.<sup>64</sup>

A closer look at Law 25326 reveals its resemblance with the European model in some capital points: the role of the informed consent,<sup>65</sup> the special regimen of treatment for sensitive data,<sup>66</sup> the presence of the major data protection principles such as the

---

<sup>61</sup> The writ of *amparo*, as stated in 43 of Argentine's constitution, has a capital role in protecting fundamental rights, as it is the only instrument able to deliver an immediate protection. v. Osvaldo Alfredo Gozaíni. *Hábeas data. Protección de datos personales*. Buenos Aires: Rubinzal – Culzoni, 2001, p. 387.

<sup>62</sup> According to Oscar Puccinelli, *habeas data* can be used in order to achieve a set of different goals, such as to access personal data, to correct it, to add to it, to update it, to delete it, to block or suspend the treatment of personal data, to eliminate the association of the data with the data' subject, among others. Oscar Puccinelli. *El habeas data en Indoiberoamerica*. Bogotá: Temis, 1999.

<sup>63</sup> Such is the evaluation of the Argentine scholars themselves. See Alejandra Gils Carbó. *Il derecho a la intimidad y ala autodeterminación informativa*. Buenos Aires: La Ley, 2001., p. 37.

<sup>64</sup> The standards of data protection in Argentina were recommended as adequate by the Article 29 Working Group in its resolution 4/2002, in October 3rd 2002, and was finally considered as adequate by European Commission in a decision of June 30th 2003.

<sup>65</sup> Además de estos principios para el tratamiento de datos personales, la existencia de consentimiento es el elemento central de la ley 25.326. Según la norma el tratamiento de datos personales es lícito cuando el titular prestó su consentimiento, que según la ley debe ser "libre, expreso e informado", y "constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias" , por ejemplo por medios electrónicos". Pablo Palazzi; Roberto Chacon de Albuquerque. "Habeas data ...", cit.

<sup>66</sup> Art. 2°. "Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual."

principle of finality, the principle of information<sup>67</sup> and the principle of proportionality.<sup>68</sup>

The Law also gave birth to an administrative office in charge of enforcing the data protection law, the DNPDP, *Dirección Nacional de Protección de Datos Personales* or National Office for the Protection of Personal Data.<sup>69</sup> This office is located inside the Ministry of Justice and, thus, cannot be held as having an independent status in the same level as its equivalents in European Union, even considering its functional autonomy.<sup>70</sup>

#### 4.2. Paraguayan System

In Paraguay the framework is not as developed as in Argentina, even if we take into account the set of legal provisions directly related to data protection in its legal system. Its 1992 Constitution recognizes in its article 33 the right to privacy in terms of the inviolability of personal and familiar intimacy,<sup>71</sup> in its article 36 the inviolability of personal documents and of their communication<sup>72</sup> and creates the *habeas data* in its

---

<sup>67</sup> Lei 25.326, art. 6°.

<sup>68</sup> Lei 25.326, art. 11, 1.

<sup>69</sup> Lei 25.326, art. 29.

<sup>70</sup> The director of DNPDP is chosen by the executive and then is approved by the senate. Lei 25.326, art. 30.

<sup>71</sup> Artículo 33 - Del derecho a la intimidad

(1) La intimidad personal y , así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. (2) Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.

Article 33 About the Right to Privacy (1) Personal and family privacy, as well as the respect of private life, are inviolable. Individual behavior that does not affect public order as established by law or the rights of third parties is exempted from the authority of public officials. (2) The protection of the privacy, dignity, and private image of each individual is hereby guaranteed (free translation by the authors).

<sup>72</sup> Artículo 36 - Del derecho a la inviolabilidad del patrimonio documental y la comunicación privada

(1) El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios.

Article 36 About the Inviolability of Personal Documents and Private Correspondence (1) Personal documents are inviolable. Records, regardless of the technique used, accountings, printed matter, correspondence, writings, telephonic communication, telegraphic communication, or any other type of communication, collections or reproductions, testimonies or objects of testimonial value, as well as their

article 135<sup>73</sup> as a writ to access personal information. There is also a data protection law, the Law 1682 of 2001, amended by Law 1696 of 2002, that states some general provisions about which data should be considered public or private and establishes a special protection to sensitive data and also presents specific measures for credit reporting, without going as far as, for instance, Argentine's law in terms of accomplishment with European standards.

#### 4.3. Uruguayan System

The recent evolution of data protection in Uruguay has been focused in modernizing its system in order to a future request of adequacy. Although the Constitution does not mention specifically privacy or data protection, it is possible to find specific sectorial rules in this sense and it should be noted that in the last years saw a series of laws regarding data protection that marked an actual evolution in the issue. In 2004 it was enacted a law that created an *habeas data* writ specifically for commercial reports,<sup>74</sup> followed by Law 17948, in 2006, which dealt with credit scoring and ultimately by Law 18331, a data protection law with general application which inspiration, in general terms, was the Spanish data protection law.

---

respective copies, cannot be reviewed, reproduced, intercepted, or seized unless a court order is issued in specific cases established in the law, and then only when action are essential for clearing up matters falling within the jurisdiction of the respective competent authorities. The law will establish special procedures for reviewing commercial accounting books and mandatory record books. (free translation by the authors).

<sup>73</sup> Artículo 135 - Del Habeas Data

Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos. Article 135 About Habeas Data Everyone may have access to information and data available on himself or assets in official or private registries of a public nature. He is also entitled to know how the information is being used and for what purpose. He may request a competent judge to order the updating, rectification, or destruction of these entries if they are wrong or if they are illegitimately affecting his rights.

Article 135 About Habeas Data Everyone may have access to information and data available on himself or assets in official or private registries of a public nature. He is also entitled to know how the information is being used and for what purpose. He may request a competent judge to order the updating, rectification, or destruction of these entries if they are wrong or if they are illegitimately affecting his rights. (free translation by the authors).

<sup>74</sup> Law n. 17838.

#### 4.4. Brazilian System

Brazil, as we said at the beginning of this session, has no general data protection regulation,<sup>75</sup> presenting only some general constitutional provisions and sectorial data protection rules. The Brazilian Constitution recognizes, in its article 5, X private life, intimacy, honor and image as fundamental rights. The same article 5 guarantees the protection of other aspects of privacy (Article 5, XI, XII, XIV),<sup>76</sup> creating in its clause LXXII a new judicial remedy, the *Habeas data*.<sup>77</sup> In the same sense the Brazilian Civil Code included in its article 21 the right to privacy as a “personality right”.

However, the only rule dealing with data protection, besides the Constitutional remedy *Habeas data* is the Brazilian Consumer Code, which articles 43 and 44 regulate the maintenance of databases and consumer files, establishing some rights for consumers.

The first of these consumer rights is the right to be communicated by the data controller<sup>78</sup> that his personal data is being processed (article 43, paragraph 2) and such

---

<sup>75</sup> In this sense are the words of Maria Celina Bodin de Moraes in the introduction she made for the portuguese translation of RODOTÀ, Stefano. *A vida na sociedade da vigilância – Privacidade Hoje*. Rio de Janeiro: Renovar, 2008. P. 12. “*A escolha brasileira, porém, ainda não está feita. Espera-se que o idêntico respeito à dignidade humana, consagrado no art. 1º, III, de nossa Constituição, bem como a tradição civilista que nosso sistema encerra, aliados à chamada globalização através dos direitos, permita a aproximação ao modelo europeu, através de uma legislação por princípios.*”

<sup>76</sup> See Privacy and Human Rights 2006. An international survey of Privacy Laws and Developments. Electronic Privacy Information Center (Washington, DC, USA) and Privacy International (London, United Kingdom). United States of America, 2006. Available at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559539](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559539). “*Article 5 of the 1988 Constitution of Brazil 1. provides that "the privacy, private life, honor and image of people are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured."* 2. *The Constitution also holds the home as "inviolable," and "no one may enter therein without the consent of the dweller, except in the event of flagrante delicto or disaster, or to give help, or, during the day, by court order."*3. *Correspondence and electronic communication are also protected, except by court order "for purposes of criminal investigation or criminal procedural finding of facts."*4. *"Access to information is ensured to everyone and the confidentiality of the source shall be safeguarded, whenever necessary to the professional activity."*5. *Finally, the Constitution provides for habeas data, which guarantees the rights: a) to ensure the knowledge of information related to the person of the petitioner, contained in records or databanks of government agencies or of agencies of a public character; and, b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative."*

<sup>77</sup> BESSA, Leonardo Roscoe. *O Consumidor e os Limites dos Bancos de Dados de Crédito*. Biblioteca de Direito do Consumidor V. 25. São Paulo: Revista dos Tribunais, 2003. P. 107.

<sup>78</sup> Although the Code establishes a common responsibility between the data controller and the supplier of goods or services that included the consumer data in a database, the Brazilian Superior Court of Justice states that the only responsible for such communication is the data controller (Digest n° 359 of the Brazilian Superior Court of Justice).

communication has to be made before such data is available in the public domain,<sup>79 /80</sup> in order to allow the consumer to exercise his rights of access and rectification, which are the other rights that article 43 guarantees.<sup>81</sup> In that sense, if the data controller does not communicate the consumer in a reasonable time, he will be able to claim for damages.

The other rights, as said above, are the rights of access<sup>82</sup> and rectification,<sup>83</sup> which means that the consumer can access any personal information stored and rectify it if he finds any inaccuracy (article 43, caption and paragraph 3). In the case that the data controller does not allow the consumer to exercise such rights, he will be able to claim damages and to exercise these through ordinary proceedings (article 43, paragraph 4) or to use the above-mentioned *Habeas data*.<sup>84</sup>

Besides, article 43 paragraphs 1 and 5 state that any negative information about the consumer, which can restrict the access to credit, shall not be stored for more than five years. Again, if the data controller fails in such obligation, the consumer will be able to claim damages and to request the exclusion of the respective negative information.

## 5. Conclusions

As has been said, there is no specific data protection regulation in Mercosur, mostly for the reason that the regional block has not reached a larger scale of integration that of a Regional Trade Agreement, since political as well as economical issues have to be solved before entering a higher level of integration. Occasionally, however, personal information has been the subject of one or another Mercosur regulation, such as the Resolution 21/04 regarding the right to information of the consumer in transactions made

---

<sup>79</sup> There is no mention in the Consumer Code about the moment in which the communication has to be done, however, both doctrine and jurisprudence are in the sense that the communication has to give the consumer enough time to exercise his rights before his personal data is available in the public domain.

<sup>80</sup> There is a local law in Rio de Janeiro that establishes the period of 10 days as a reasonable one (Law n° 3.244, 6 September 1999). Available at <http://www.alerj.rj.gov.br/processo2.htm> (28/09/08).

<sup>81</sup> BENJAMIN, Antônio Herman de Vasconcellos et al. Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto. P. 405.

<sup>82</sup> BENJAMIN, Antônio Herman de Vasconcellos et al. Cit., P. 413.

<sup>83</sup> BENJAMIN, Antônio Herman de Vasconcellos et al. Cit., P. 416.

<sup>84</sup> The proceedings of *Habeas data* remedy were regulated by Federal Law n° 9.507, 12 November 1997. Available at [http://www.planalto.gov.br/ccivil\\_03/Leis/L9507.htm](http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm) (20/09/08).

through Internet, which article 3 mentions the need of a privacy policy to be presented by the seller when trading on-line and collecting personal information.

The issue of adequacy to European Union standards drove the legislator of Argentina and, most recently, of Uruguay, to adopt a general data protection law tailored to suit both their own needs but also very carefully trying to maintain a degree of resemblance with the European standards. The same does not seem to apply neither for Paraguay nor for Brazil, both countries that officially have not moved (at least not yet) into this direction. The case of Brazil is somewhat interesting because the country, even having been a pioneer when first introduced the *habeas data* writ, has not developed its own data protection framework towards its recognition as a fundamental right, nor has any attempt of adopting any kind of general data protection law in the sooner future.

Mercosur has undoubtedly a very important role helping its Member States to reach a certain degree of harmonization of its law and surely data protection can be a key issue as it represents an element of both internal and external integration. The internal integration has to do with the reduction of commercial costs as a result of all Mercosur's Member States sharing the same core principles in their data protection law, giving one Member State's citizen to have the same expectancy of privacy regarding his personal data wherever in Mercosur. The external integration comes also as a result of this common data protection framework and can be seen as the increase on the competitiveness of the Member State's markets as a whole, as they are more likely to make deals with other countries which legislation blocks the transfer of personal data to places where it cannot be reasonably protected (the typical case of European countries).

It can't be emphasized enough how much the atypical nature of data protection makes it play a very distinctive role whenever it becomes part of a law system. Its international nature was mentioned, its double nature of being both a fundamental right and a tool that can provide a certain harmony in the market too (it has been even symbolically to Janus, the Roman god with two distinct heads). In the specific case of Mercosur and considering some of its inherent deficits, as the difficulties faced when trying to enforce closer commercial ties or even the distance between Mercosur itself and the citizen of its Member States, data protection can be specifically useful to achieve some desirable goals: (i) set the experience of integration to another level by enforcing

the data protection as a commercial need but, at the same time, accomplishing a general benefit to Mercosur's citizens by granting a higher level of protection to their personal data; (ii) promote the citizen's trust in Mercosur by enacting rules about data protection that can affect positively their rights and so improving the relation between the block and the individual. In doing so it can become possible to experience an actual case of integration through the citizenship and the respect of fundamental rights in a way that goes beyond the mere rhetoric or, as once mentioned by Stefano Rodotà in another sphere, a kind of globalization through Law.

The means to do so are certainly all but certain, but surely the first steps were already taken by the Argentine Republic when proposing a Treaty for personal data protection in Mercosur in 2004. Apart the challenges in enacting such a piece of legislation that has effects in zones not yet covered by the norms already enacted by Mercosur, it is convenient to suggest some procedures that could help the discussion and implementation of such a treaty, such as: (i) The adoption of a specific agenda that recognizes the problems the countries in the block face related to data protection and establishes a set of data protection principles to be observed as a starting point to the harmonization of each country's internal law in this issue, and (ii) the creation of an Mercosur office or organ in charge of the enactment of these principles. The pertinence of the issue of data protection and its importance both to Mercosur's as to their citizen's fundamental rights seems to be also an excellent opportunity to project Mercosur's future.